Return to Menu

Part No. P0937241 02.1

Business Communications Manager 2.5

Programming Operations Guide

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. July, 2001.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Software licensing

The Apache Group

Copyright (c) 1995-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the Apache Group for use in the Apache HTTP server project (*http://www.apache.org/*)."
4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission.

   For written permission, please contact *apache@apache.org*.
5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the Apache Group for use in the Apache HTTP server project (*http://www.apache.org/*)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Group and was originally based on public domain software written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Group and the Apache HTTP server project, please see *http://www.apache.org/*.

Info-ZIP

Copyright (c) 1990-2001 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

> Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Contents

Software licensing 3
The Apache Group 3
Info-ZIP 4
Preface 35
Before you begin 35
Symbols used in this guide 36
Text conventions 36
About the buttons on your telephone 37
Acronyms 38
Related publications 41
How to Get Help 42
Chapter 1
Introduction 43
System Hardware 47
Business Communications Manager Software 47
How Does the Network Work? 48
What Do Modules Do? 48
Chapter 2
Getting Started With Unified Manager 49
Computer requirements 49
Browser Requirements 49
Using a HTTP Proxy server 50
To Bypass the HTTP Proxy on Microsoft Internet Explorer 5.0 50
To Bypass the HTTP Proxy on Netscape Communicator 4.5 50
Logging on to Unified Manager 51
Using the Unified Manager Buttons 51
Using the Configure Button 52
Using the Preinstalled Client Access Home Page hyperlink 52
Installing the Java Class Files on Your Computer 53
Logging on Using the Preinstalled Client Access Home Page 53
Using the Configure Button Features to Manage the System 54
Managing Data Networking on the System 54
Managing the Telephony System 54
Managing Business Communications Manager Optional Features 54
Finding Documentation 54
Using BRU 54
Maintaining Your System 55

Logging Off the Unified Manager 55
Using the Unified Manager 55
Business Communications Manager System Access 55
Unified Manager Display 56
Understanding the Dynamic Menu 57
Understanding the Navigation Tree Headings 57
Understanding Tabbed Pages 58
How This Guide Uses the Navigation Tree 58

Chapter 3
Configuring Start-up System Parameters 59

Warnings 59
Accessing the Wizards 60
About the Other Wizards 60
Navigating the Wizards 61
Configuring Your System with the Quick Start Wizard 62
What You Need to Know 63
Entering Information in the Quick Start Wizard 64

Chapter 4
Telephony Services Overview. 65

Planning 68
Information Matrices 69
Networking Systems 69

Chapter 5
Configuring Resources — Media Bay Modules. 71

About the Media Bay Module Records 71
Media Bay Module Bus Numbers 72
Ports on Bus Heading 73
Module # Heading 73
Notes About Media Bay Module Buses 73
Configuring Media Bay Modules 74
Identifying the Module 74
Defining Trunk Module Types and Settings 76
Determining Clock Sources for DTMs or BRIs 80
T1 Interface Parameters (region-specific) 81
E1 Parameters (region-specific) 83
PRI Call-by-call Service Selection 83
Provisioning lines (PRI, T1, & DASS2) 85
Deprovisioning a line/loop 86
Configuring DECT Resources 87

DECT Documentation 88
Enabling or Disabling Modules 88
Disabling a Bus 88
Disabling a Single Module 88

Chapter 6
Configuring Lines, Loops, and Routes 91

Configuring Line Settings 91
Copying Data to Other Lines 92
Determining Which Lines You Need to Program 92
VoIP Lines 92
Target Lines 93
Physical Lines 93
All Lines 95
Configuring Line Records 96
Using the General Record 96
Assigning Trunk/line Data 97
Assigning Restrictions 103
Line Restrictions 103
Remote Restrictions 104
Telco Features 104
Line Matrix 105
Configuring Loops 106
Configuring the LoopType 107
SPIDs (NI only) 108
Assigning the Number of B channels 108
Assigning DNs 109
Assigning Call type for a Network DN 109
Loop Matrix 109
Determining Line Access 109
Configuring Access Codes 111
Programming Access Codes 111
Tips About Access Codes 112
Line Pool Access Codes 114
Using Carrier Codes 115
About Carrier Access Codes 115
Identifying Carrier Access Codes 115
Access Code Matrix 116
Configuring Call Routing 117
About Call Routing 117
Routes and Destination Codes 118
Avoiding Routing Conflicts 119

Defining Routes 119
Call by Call Service Routing 120
Programming the PRI Routing Table 121
Programming Destination Codes 122
Wild Card Character 122
Setting Up a Route for Local Calling 124
Setting Up a Route for Long Distance Calling 125
Adding a Long Distance Carrier Access Code 126
Programming for Least Cost Routing 127
Overflow Routing 127
Using Dialing Restrictions with Routing 128
Using a Dialing Plan to Route Outgoing PRI Calls 128
Enbloc Dialing 128
Routing Matrix 129
System Line Settings 129
Network Name Display 129
Receiving and Sending Calling Party Name 130
Network Name Display interactions 130
Programming Network Name Display 130
Remote Access Line Settings 131
Remote Access on Loop Start Trunks 131
Remote Access on a Private Network 131
Remote Access on T1 DID Trunks 132
Remote Access on PRI Trunks 132
Remote Access on DPNSS Lines 132

Chapter 7
Configuring System DNs 135

About System DNs 135
Identifying System DNs 136
Active Set DNs 136
Active Companion DNs 137
Active Application DNs 137
Inactive DNs 137
All ISDN/DECT DNs 138
All System DNs 138
Feature DNs 139
Using a Wizard to Renumber Telephone DNs 139
Change Telephone DNs Using the Unified Manager 140
Using Wizards to Control DN Records 140
Creating User Templates with the Edit Template Wizard 140
What You Need to Know 141

Using the Edit Template Wizard 143
Creating Telephone Records with the Add Users Wizard 143
What You Need to Know About the User 144
Using the Add Users Wizard 146
System DNs Headings and Features 147
Copying Settings to Other DNs 148
Identifying the Telephone (General Heading) 149
Using the Line Access Heading 150
Assigning Line Access 150
Determining Line Assignments 152
Applying Target Lines 152
Assigning Outgoing Lines 153
Assigning Line Pool Access 155
About PRI Line Pools 155
Using Answer DNs 155
Assigning Answer DNs 156
Defining Capabilities 157
Assigning Call Forward 158
Assigning a Hotline 159
Determining ATA Settings (Analog Telephones) 160
Setting Intrusion Controls 161
Defining User Preferences 162
Programming Telephone Buttons 163
Assigning User Speed Dials 164
Programming Restrictions 165
Defining Set Restrictions 165
Setting Restriction Schedules for Telephones 167
Defining Line/set Restrictions 167
Configuring Telco Features 169
Digital Telephones DN Record Matrices 170
Setting CAP Assignments 174
Configuring a CAP assignment 174

Chapter 8
Controlling Access to the System 175

DN Lengths 175
Direct Calling from Inside and Outside the System 177
Creating Direct Dial Sets 177
Direct Dial Matrix 178
Creating Target Lines 178
Target Lines Matrix 179
Creating Direct Inward System Access (DISA) 180

Using Dialing Plan Settings 180
Dialing Timeout 180
Using Private Networking Dialing Plans 181
Setting up Public Network Dialing 181
About the Public DN LengthsTable 182
Adding or modifying Public DN lengths 182
Dialing Plans Matrix 183
Configuring Remote Access 183
Remote Access Packages 183
Defining Line Pool Access for Remote Packages 184
COS Passwords 184
Remote Access Matrix 185
Configuring Call by Call Limits 186
Supporting protocols 186
Call by call services 186
Switches Supporting Call by Call Limits 187
Provisioning for Call by Call Limits with PRI 188
Other Required Programming in the Unified Manager 188
Setting CbC Limits 188
PRI Line Pools 189
CbC Matrix 189
Defining Restriction Filters 190
Notes About Restriction Filters 190
Programming a Restriction Filter 193
Default Filters (North America) 194
Restriction Filters Matrix 195

Chapter 9
Configuring Public Networks 197

Simple Networking 197
Call Access to the Business Communications Manager 197
Callers Using Business Communications Manager 198
Callers in the Public Network 198
Callers in the Private Network 198
Dialing Plans for T1 Lines 198
Dialing Plan Using Public Lines 199
Destination Code Numbering in a Network 200

Chapter 10
Configuring Private Networks. 201

Private Networking Protocols 201
Keycode Requirements 201

Remote Access to the Network 201
Lines Used for Networking 202
Using Routing to Create Networking With T1 E&M Lines 203
Using Shared Line Pools to Create a Network 206
PRI networking using Call-by-Call Services 208
Private networking with PRI SL-1 211
System Numbering Plans 211
Creating Tandem Private Networks 212
Routing for Tandem Networks 217
Using SL-1 with MCDN to Network with a Meridian System 219
Meridian System Requirements 219
Meridian MCDN Features 219
Creating an SL-1 Network 227
Business Communications Manager Module Settings 229
Business Communications Manager Dialing Plan Settings 229
Business Communications Manager Routing Information 230
Networking with ETSI QSIG 231
Hardware programming for the branch offices 232
ETSI Network Services 232
DPNSS 1 Services 234
DPNSS 1 Capabilities 234
DPNSS 1 Features 235
Three Party Service 235
Making a Conference Call 236
Using the Diversion Feature 236
Restrictions by Telephone Type 237
Setting Diversion 237
Using the Redirection Feature 237
Restrictions by Telephone Type 238
Setting Redirection 238
Executive Intrusion 238
Restrictions by Set Type 238
Intrusion Levels 238
Call Offer 239
Displays 239
Restrictions by Telephone Type 240
User Actions 240
Route Optimization 240
Setting Route Optimization 241
Message Waiting Indication 241
Restrictions by Set Type 241
Setting Message Waiting Indication 242

Assigning Message Centers to a Line 242
Programming MWI and MWC 243
Selecting a Message Center 243
Setting Message Waiting Indication 244
Loop Avoidance 244
Programming Loop avoidance 244
Private Networking with DPNSS 245
Guidelines for Creating a Private Numbering Plan with DPNSS 247
Customizing the Routing Service 247
VoIP Networking 248

Chapter 11
Configuring System Settings 249

Scheduled Services Headings 249
Common Settings 250
Defining the Service Control Password 250
Changing Schedule Names 250
Schedule Times 251
About Start and Stop Times 251
Programming Scheduled Services 252
Ringing Service 253
Ring Groups 253
Schedules 253
Line Settings 254
Restriction Service 255
Routing Service 256
Services Matrix 257
General Settings 259
Business Name 260
Feature Settings 260
Phantom DNs 262
SWCA Controls 263
Call Log Space 264
System Features Matrix 264
Timers 265
Timers Matrix 266
Release Reasons 266
System Speed Dial 267
Adding or Changing a System Speed Dial 267
Creating a System Speed Dial 267
System Speed Dial Matrix 268
Telco Features 269

Voice Message Center Numbers 269
ONN Blocking 270
Configuring ONN 270
Telco Features Matrix 271
Enhanced 911 (E911) Configuration 271
911 and IP telephones 272

Chapter 12
Configuring Portable Services 273

Companion Wireless System 273
Registering Companion Handsets 274
Using Portable DNs to Show Handset Status 275
Deregistering a Handset 275
Defining Radio Data 276
Programming Base Station Radios 276
Defining Cells 277
Registering Companion Portables 277
Portable Telephone Programming 278
Companion Matrix 280
DECT Portable Systems 281
DECT Matrix 281
Programming for Mobile Handsets 282

Chapter 13
Configuring Hunt Groups 285

How Hunt Groups Work 286
Identifying a Hunt Group 286
Hunt Group Members 288
Adding a Hunt Group Member 288
Removing a Hunt Group Member 289
Removing All Members from a Hunt Group 289
Moving Members of a Group 289
Programming Hunt Group Lines 290
Assigning or Unassigning Lines to a Hunt Group 290
Assigning a Line 290
Unassigning a Line 290
Unassigning All Lines 291
Hunt Group Tips 291
Feature Operation Within Hunt Groups 291
Hunt Group Matrix 292

Chapter 14
Configuring Hospitality Services 293

About the Hospitality Feature 293
Hospitality Telephone Definitions 294
Alarm Time (AL) Feature 294
Power Failures 294
Setting Up the Hospitality System 295
Identifying Room Sets 296
Identifying Call Permissions 296
Setting Room Restriction Filters 297
Alarm Data 297
Setting Alarm Parameters 297
Expired Alarms 298
Hospitality Matrix 298

Chapter 15
Configuring the MSC resources 299

Types of MSC resources 299
Rules for managing the MSC resources 300
Signaling channel rules 300
Media channel rules 301
Example of how to estimate peak media channel usage 301
DSP resources rules 302
Voice bus path 303
Media gateways 303
Determining the MSC resources you require 303
Evaluation 308
Example of a Business Communications Manager configuration 309
Configuring the MSC resources 310
Viewing the MSC information 310
Viewing the MS-PEC configuration 310
MSC Configuration 312
Viewing the MSC Configuration 313
Changing the MSC configuration 313
Creating a custom MSC configuration 314
DTMF Configuration 316
Changing the DS30 Split 316

Chapter 16
Configuring Business Communications Manager Data Networking Resources319

Viewing Business Communications Manager resources 319
LAN 320

Viewing the LAN resources . . . 320
Configuring LAN resources . . . 320
Setting LAN global parameters . . . 320
Configuring a LAN interface . . . 321
Configuring multiple IP addresses for the LAN interface . . . 323
Viewing LAN performance . . . 325
WAN . . . 326
Permanent WAN Connection . . . 326
Frame Relay . . . 326
Point-to-Point-Protocol (PPP) . . . 326
Multi-link Point-to-Point Protocol (MLPPP) . . . 327
WAN Data Compression . . . 327
Viewing WAN Resources . . . 327
Setting global WAN parameters . . . 327
Configuring WAN Summary Parameters . . . 329
Setting WAN Line Parameters . . . 330
Setting WAN Sync Parameters . . . 331
Setting WAN Frame Relay Parameters . . . 331
PVC Congestion Control . . . 333
To add PVC congestion control: . . . 333
To modify a PVC congestion control entry: . . . 334
To delete a PVC congestion control entry: . . . 334
WAN PPP Parameters . . . 335
Configuring multiple IP addresses for the WAN interface . . . 335
WAN performance . . . 337
Dial Up . . . 338
Configuring the Dial Up Global parameters . . . 338
V.90 modem (North America) Dial Up . . . 338
Configuring V.90 modem interface for dial up WAN backup connection . . . 339
ISDN Dial Up . . . 341
Creating an ISDN dial up interface . . . 341
Configuring an ISDN interface . . . 342
ISDN Channel Characteristics . . . 344
Deleting an ISDN interface . . . 345
Point to Point Protocol on Ethernet (PPPoE) . . . 346
Enabling PPPoE . . . 346
Creating a PPPoE dial up interface . . . 347
Configuring PPPoE . . . 347
Deleting an PPPoE interface . . . 349
Guidelines for using Remote Dial-in . . . 350
Configuring a data module . . . 350
Viewing the data module settings . . . 350

Programming the BayStack settings 350
Fixed access 351
Switched access (PRI & BRI) 351
Line assignment 351
Line pool access 352

Chapter 17
Configuring Business Communications Manager Data Services 353

Programming Data Services 353
DHCP 354
Configuring the DHCP Mode 355
Configuring a DHCP server 355
LAN settings for DHCPServer 357
Address ranges 358
Excluded addresses 360
Reserved Addresses 361
Remote Scope 363
Adding a remote scope 363
Remote scope settings 363
Deleting a Remote Scope 368
Configuring a DHCP Relay Agent 368
LAN settings for DHCPRelayAgent 369
Importing and Exporting DHCP data 370
Exporting DHCP data 370
Importing DHCP data 371
DNS 372
Guidelines for using Business Communications Manager DNS service 372
IP Routing 374
Routing Information Protocol (RIP) 374
Open Shortest Path First (OSPF) 374
Configuring IP Routing 375
IP Routing global settings 375
Setting the RIP Global Settings 376
Setting the OSPF Global Settings 376
Configuring IP routing on an interface 377
Configuring RIP parameters on a network interface 377
Configuring OSPF Parameters on a network interface 379
OSPF NBMA Neighbors 381
Static routes 382
IPX Routing 384
Enabling IPX Routing 384
Configuring IPX Routing 385

Configuring Packet Filters for IPX routing 387
Adding Packet Input filters 387
Modifying Packet Input filters 388
Deleting Packet Input filters 389
Adding Packet Output filters 389
Modifying Packet Output filters 390
Deleting Packet Output filters 390
RIP filters for IPX routing 390
Configuring RIP for IPX Routing 390
Adding RIP Input Filters 392
Modifying RIP Input filters 393
Deleting RIP Input filters 393
Adding RIP Output filters 393
Modifying RIP Output filters 394
Deleting RIP Output filters 394
SAP filters for IPX routing 395
Configuring the SAP for IPX Routing 395
Adding SAP Input Filters 396
Modifying SAP Input Filters 397
Deleting SAP Input Filters 397
Adding SAP Output Filters 398
Modifying SAP Output Filters 398
Deleting SAP Output Filters 398
Static Routes for IPX Routing 399
Adding Static Routes for IPX Routing 399
Modifying Static Routes for IPX Routing 400
Deleting Static Routes for IPX Routing 400
Static Service for IPX Routing 400
Adding a Static Service for IPX Routing 400
Modifying a Static Service for IPX Routing 401
Deleting a Static Service for IPX Routing 401
SNMP 403
Guidelines for using SNMP 403
Configuring SNMP 403
SNMP Community List 404
Adding a community to the list 404
Modifying a community 404
Deleting a community 405
Manager List 405
Adding a manager to the Manager List 405
Modifying a manager 406
Deleting a manager 406

Trap Community List 406
Adding a trap community to the Trap Community List 406
Modifying a trap community 407
Deleting a trap community 407
QoS monitor 408
QoS Monitor Mean Opinion Score 408
Web cache 410
Guidelines for using Web Caching/Proxy 410
Net Link Manager 412
Selecting a permanent WAN link as the primary WAN connection 413
Selecting a dial-up link as the primary WAN connection 414
Alarm Service 415
NAT (Network Address Translation) 416
Static NAT 416
Dynamic NAT 416
NAT and IP Firewall filters 416
Managing Business Communications Manager 417
Enabling and disabling NAT 417
Configuring an Interface with NAT 417
Adding Default rules 417
Adding a Rule to an interface 418
Modifying a Rule to an Interface 419
Deleting a Rule to an Interface 419
Configuring the Rule order 420
Examples of common NAT configurations 420
NTP Client settings 422
Configuring the NTP Client settings 422
Starting the NTP Client Service 423

Chapter 18
Virtual Private Networks (VPN) 425

PPTP 426
Settings required for PPTP tunnels 426
NAT (Network Address Translation) 426
QoS 426
IP Routing and IPX Routing 427
Filters 427
IP Addresses and DHCP Server 427
DNS Server 427
Changing the PPTP settings 428
Adding a PPTP Client 429
Deleting a PPTP client 429

Adding a PPTP tunnel 430
Configuring a PPTP tunnel 431
To add a Destination Network 433
To modify a Destination Network 434
To delete a Destination Network 434
Deleting a PPTP tunnel 435
IPSec 436
Encryption 436
Protocol 437
Encryption method 437
Authentication method 438
Settings required for IPSec tunnels 438
NAT (Network Address Translation) 438
Filters 438
Routing 438
Dialup ISDN connections 438
Compatibility with Contivity Extranet Switch and Shasta 5000 439
IPSec and PPTP 439
Changing the IPSec global settings 439
Adding an IPSec Tunnel 440
Adding Local Accessible Networks to the IPSec tunnel 441
Adding Remote Accessible Networks to the IPSec tunnel 442
Modifying an IPSec Tunnel 443
Modifying Local Accessible Networks to the IPSec tunnel 443
Modifying Remote Accessible Networks to the IPSec tunnel 443
Deleting an IPSec Tunnel 444
Deleting Local Accessible Networks to the IPSec tunnel 444
Deleting Remote Accessible Networks to the IPSec tunnel 444
Creating a tunnel between two Business Communications Manager systems 445
On the first Business Communications Manager: 445
On the second Business Communications Manager: 445
Creating a tunnel between a Business Communications Manager and a Contivity Extranet Switch v02_61 446
On the Business Communications Manager: 446
On the Contivity Extranet Switch: 446

Chapter 19
Policy-enabled networking 447

Overview 447
Differentiated Services (DiffServ) overview 447
DiffServ IP Quality of Service (QoS) architecture 447
DiffServ components 449

IP service classes 449
Packet classifiers 450
COPS 451
Policy overview 451
Implementing Quality of Service (QoS) 453
Configuring the QoS Summary parameters 453
Configuring Devices 455
Creating an interface group configuration 455
Modifying an interface group configuration 455
Deleting an interface group configuration 456
Configuring Rules 456
Creating an IP filter configuration 456
Modifying an IP filter configuration 458
Deleting an IP filter configuration 458
Creating an IP filter group entry 458
Modifying an IP filter group configuration 459
Deleting an IP filter group entry 459
Configuring Actions 460
Creating an Action 460
Modifying an Action entry 460
Deleting an Action Entry 461
Configuring QoS policies 461
Adding a policy 461
Modifying a policy 462
Deleting a policy 462
Implementing Common Open Policy Services (COPS) 463
Viewing COPS statistics and capabilities 463
Configuring a COPS Client 466
Adding a COPS Client Server entry 466
Modifying a COPS Client Server entry 466
Modifying the COPS Client Server Retry Data 467
Configuring the Policy Agent characteristics 468
IP Firewall Filters 470
Packet filtering 470
Basic (stateless) Packet Filter 470
Stateful Packet Filters 470
IP Firewall filters and NAT 471
Viewing and changing the status of Firewall Filters 471
Configuring IP Firewall Filters for an interface 471
Adding Default Rules 472
Adding an Input Filter for a Firewall Filter Interface 473
Modifying an Input Filter for a Firewall Filter Interface 474

Deleting an Input Filter for a Firewall Filter Interface 475
Configuring the order of the Input Filters for an interface 475
Adding an Output Filter for a Firewall Filter Interface 475
Modifying an Output Filter for a Firewall Filter Interface 475
Deleting an Output Filter for a Firewall Filter Interface 476
Configuring the order of the Output Filters for an interface 476
Accessing Unified Manager through the Firewall 476

Chapter 20
Configuring Management Settings. 479

User Manager 479
Adding a user profile 480
Modifying a user profile 480
Deleting a user profile 481
Alarm Manager 481
Configuring the Alarm Manager 482

Chapter 21
Backup and Restore Utility (BRU) 485

Starting BRU 485
Backing up Business Communications Manager settings 486
Restoring Business Communications Manager settings 488
Scheduling a backup 489
Viewing the scheduled backups 490
Viewing a scheduled backup report 491
Deleting a scheduled backup 491
Administering backup volumes 491
Adding volumes 491
Modifying volumes 492
Deleting volumes 492
Saving a backup job 493
Loading a saved backup job 493
Deleting a saved backup job 493
Transferring a file 494
Resetting the BRU screen 494
Exiting from BRU 495

Chapter 22
Maintenance 497

Business Communications Manager general maintenance 497
System startup 497
Warm reset 498

Business Communications Manager system diagnostics and utilities 498
Performance Statistics 498
Generating System Performance Statistics 499
Error Messages 499
User Actions 499
Errors List 500
MIB II Information 503
Counters Shown at LAN and WAN Interface Levels 503
ICMP Counters 504
UDP Counters 505
TCP Counters 505
QoS Session Counters 505
QoS Best Effort Traffic Counters 506
QoS Dropped Packets Counters 506
QoS Graph Counters 506
QoS Best Effort Queue Counters 506
Maintenance programming for telephony resources 507
System version 507
Media Bay Module status 508
Display the Media Bay Module status 508
Disable a module 508
Enable a module 509
Identify a device connected to the system 509
Disable a device 510
Enable a device 510
System test log 511
Display information on the items in the System test log 511
Erase the log 511
System administration log 512
Display information on the items in the System Administration log 512
Erase the log 513
Network event log 513
Displaying information on the items in the Network event log 513
Erase the log 514
Alarm codes 514
Event messages 515
Significant event messages 515
How to read an event message 517
Events that cause a system restart 518
Companion event messages (North American systems only) 519
Tests 523
Line loopback test 523

Payload loopback test 524
Card loopback test 524
Continuity loopback test 524
Start a loopback test 524
DN-to-port conversion 525
Debug 525
CSU statistics 526
Statistics collected by the Business Communications Manager system 526
Enable the internal CSU 527
Check the performance statistics 527
Check the CSU alarms 528
Check carrier failure alarms 528
Check bipolar violations 528
Check short term alarms 528
Check Defects 529
Reset all statistics 529
Link Status 529
Metrics 530
CbC limit metrics 530
Hunt Group Metrics 530
PSTN fallback metrics 530
Moving telephones 531

Chapter 23
Troubleshooting your Business Communications Manager system 533

General troubleshooting information 533
Getting ready 534
Types of problems 534
Basic troubleshooting procedure 534
Viewing system performance and fault alarms 535
System performance graphs and tables 535
Fault Alarm Banner 535
Alarm Browser 536
Problems with telephones 536
Digital telephone display is unreadable 536
Telephone has no dial tone 537
Problems with lines 537
Calls can be received but cannot be made 538
Dial tone is absent on external lines 538
Lines at a telephone are busy after call is over 539
A redirected line remains busy 539
Programming is incorrect 539

Lines require maintenance session 540
Auto-answer line rings at a telephone 540
Installed hardware does not support disconnect supervision 540
Line is configured as auto-answer and unsupervised 540
Line is not equipped for disconnect supervision at the central office 541
Trunk module's disconnect timer setting is not correct 541
Prime telephone gets misdialed calls 541
Selected line reads "Not in service" or "Not available" 541
Line is connected to a DTM which is currently not in service 542
Line has been disabled for maintenance purposes 542
Line has not been provisioned 542
Selected line pool shows "No free lines" 542
Problems with optional equipment 543
Problems with the ATA 2 543
Running a Maintenance session to test a ATA 2 543
Problems with the auxiliary ringer 544
Problems with external paging 544
Problems with Music on Hold and Background Music 544
Problems with module service 545
Digital Trunk Module trouble 546
Monitoring the T1 or PRI signal 547
Problems with Trunk or Station Modules 547
Problems for network or remote users 548
Remote feature code gets no response 548
Dialed number gets ringback and the wrong person 548
Dialed number gets dial tone instead of ringback 549
Dialed number gets busy tone 549
Dialed number does not get through 549
Digits do not match Received number or Auto DN 549
The Business Communications Manager system did not receive some or all of the incoming digits 550
Dialed feature code gets overflow tone 550
Remote caller does not have access to that feature 550
Feature code is not valid 550
Call may originate on a telephone that uses pulse signaling 550
Dialed feature code gets busy tone 551
Line pool access code gets overflow tone 551
Remote caller does not have access to line pool 551
Line pool access codes are invalid 551
Call may originate on a telephone that uses pulse signaling 551
Line pool access code gets ringback 552
Line pool access code gets busy tone 552

Dialed number gets no response 552
Remote caller dials before far end is ready 552
Line malfunction 552
System malfunction 552
Problems with Companion sets 553
Rebooting the Business Communications Manager server 553
Shutting down Business Communications Manager system 553

Appendix A
Setting Up Remote Routers for IP Telephony prioritization 555

Creating an Outbound Traffic Filter 555
Sample Criteria, Ranges, and Actions for UDP Filtering 556

Appendix B
ISDN Overview 557

Welcome to ISDN 557
Analog Versus ISDN 557
Types of ISDN Service 558
ISDN Layers 558
ISDN Bearer Capability 559
Services and Features for ISDN BRI and PRI 559
PRI Services and Features 559
BRI Services and Features 560
ISDN Hardware 563
PRI Hardware 563
BRI Hardware 563
Clock Source for ISDN 565
ISDN BRI NT1 equipment 566
ISDN Standards Compatibility 566
Planning your ISDN network 566
Ordering ISDN PRI 567
Ordering ISDN BRI 567
Supported ISDN Protocols 568
ISDN Programming 569
Program PRI Resources 569
Programming ISDN BRI Resources 569
Program PRI Lines 571
Program ISDN BRI Lines 571
Program Direct Inward System Access (DISA) on PRI Lines 571
Program ISDN Equipment 572

Appendix C
Region-based System Settings 575

Core Software and Regions 575
Languages 576
Caller ID Displays 577
Companding Law by Region 577
ISDN Line Services 578
Mobility Services by Region 579
Media Bay Module Availability by Region 580
Trunk Availability by Region 581
BRI and PRI line types 583
Defining Time Zones by Country and Language 585
System Defaults 586
Voice Mail Regions 589

Appendix D
Button programming: Features 593

Glossary 597

Index 633

Figures

Figure 1 Process for installing the telephony components 44
Figure 2 Process for installing the data component 45
Figure 3 Process for activating optional features 46
Figure 4 Unified Manager first-page buttons 51
Figure 5 Main display of the Unified Manager 56
Figure 6 Lines menus and fields 58
Figure 7 Tasks for installing the telephony components 66
Figure 8 Telephony Services menu options 67
Figure 9 Resources/Media Bay Modules menus 72
Figure 10 Confirming the Programmed Bus Type 74
Figure 11 Example of PRI module settings 77
Figure 12 DECT Media Bay Module description 87
Figure 13 DECT maintenance selection 87
Figure 14 Lines menus and fields 91
Figure 15 Loops headings. 106
Figure 16 Describing line management 110
Figure 17 Call Routing headings 117
Figure 18 Routing Service programming example 124
Figure 19 Destination codes for call routing 125
Figure 20 Carrier code call numbering sequence 126
Figure 21 System DNs main headings 136
Figure 22 DN headings and features 147
Figure 23 Assigning a line to a set 178
Figure 24 Defining a Received number 179
Figure 25 Restriction Filters headings 190
Figure 26 Line restriction example 192
Figure 27 Remote line restriction example 192
Figure 28 Connection to a private network 197
Figure 29 Routing service record: use pool 199
Figure 30 Routing service record: Destination code 199
Figure 31 Dialing plan for Business Communications Manager network 203
Figure 32 Network example using shared line pools 207
Figure 33 PRI networking using Call-by Call Services 209
Figure 34 Private tandem network between systems 212
Figure 35 Network call transfer from a Meridian system 220
Figure 36 Network call redirection path 221
Figure 37 Message waiting indication message 221
Figure 38 Call loop on system without ICCL 222
Figure 39 Call paths with and without TRO 223

Figure 40 Call paths with and without TRO 224
Figure 41 Camping a call 225
Figure 42 Breaking into a Business Communications Manager call path 226
Figure 43 MCDN networking, with a common public network connection 228
Figure 44 ETSI QSIG networking 231
Figure 45 DPNSS networking 246
Figure 46 Scheduled Services headings 249
Figure 47 General Settings headings and fields 259
Figure 48 System speed dial headings 267
Figure 49 Telco features headings for voice messaging and ONN 269
Figure 50 Companion headings 273
Figure 51 Hunt groups menus and fields 285
Figure 52 Hospitality commands and settings 293
Figure 53 Hospitality commands and settings 319
Figure 54 DiffServ bandwidth brokers and nodes 448
Figure 55 S reference point 564
Figure 56 T reference point 565

Tables

Table 1 Telephone buttons . . . 37
Table 2 Navigation tree menu functions . . . 57
Table 3 Telephony Services sub headings . . . 68
Table 4 Module/Offset correlations . . . 73
Table 5 Programmed Bus Types . . . 75
Table 6 Bus XX record settings . . . 76
Table 7 Module record values . . . 78
Table 9 TI parameters . . . 82
Table 10 Services available for each PRI protocol . . . 84
Table 11 Module record values . . . 84
Table 12 Bus/line-loop default list . . . 93
Table 13 General record values . . . 96
Table 14 Line settings table . . . 98
Table 15 Default restriction filters . . . 103
Table 16 Default remote restrictions . . . 104
Table 17 Line attributes . . . 105
Table 18 Loop settings . . . 107
Table 19 Loop attributes . . . 109
Table 20 Default codes table . . . 111
Table 21 Access codes values . . . 112
Table 22 Carrier access code values . . . 115
Table 23 Access code values . . . 116
Table 24 Avoiding code conflicts . . . 119
Table 25 Route settings . . . 120
Table 26 Call by Call routing table example . . . 120
Table 27 Destination codes without wild cards . . . 123
Table 28 Routing . . . 129
Table 29 Call features/interface list . . . 129
Table 30 Default DNs, based on assigned bus number . . . 138
Table 31 General record values . . . 149
Table 32 Telephone line access fields. . . . 151
Table 33 Telephone line assignment fields . . . 153
Table 34 Answer DN settings . . . 156
Table 35 Capabilities fields . . . 157
Table 36 Call forward fields . . . 158
Table 37 Hotline values . . . 159
Table 38 ATA settings . . . 160
Table 39 User preference choices . . . 162
Table 40 Button programming choices . . . 163

Table 41 User speed dial settings . . . 165
Table 42 Telephone restriction fields . . . 166
Table 43 Schedule filter defaults . . . 167
Table 44 Telco features settings . . . 169
Table 45 DN equipment identification . . . 170
Table 46 General and Line access settings for DNs . . . 170
Table 47 Capabilities . . . 171
Table 48 User preferences . . . 172
Table 49 Button programming . . . 172
Table 50 User speed dial settings . . . 172
Table 51 Telephone (set) Restrictions . . . 172
Table 52 Telephone restriction schedules and line/set restrictions . . . 173
Table 53 DN record, Telco features . . . 173
Table 54 DN length values . . . 176
Table 55 Received # length values . . . 176
Table 56 Direct dial values . . . 177
Table 57 Direct dial sets . . . 178
Table 58 Target line record . . . 179
Table 59 Private network values . . . 181
Table 60 Dialing plan matrix . . . 183
Table 61 Private network values . . . 183
Table 62 COS password values . . . 185
Table 63 Remote access matrix . . . 185
Table 64 Call by Call Services available on the system . . . 186
Table 65 Switches and service types chart . . . 187
Table 66 DN length values . . . 188
Table 67 CbC matrix . . . 189
Table 68 Default restriction filters . . . 194
Table 69 Default filters for program headings . . . 194
Table 70 Restriction filters matrix . . . 195
Table 71 Destination code leading digits . . . 200
Table 72 E&M routing for a Business Communications Manager network . . . 203
Table 73 Creating a coordinated dialing plan using line pools . . . 207
Table 74 PRI call-by-call services routing information . . . 210
Table 75 Call originating from the public network to a tandem network . . . 213
Table 76 Calls originating from the private network within a tandem network . . . 215
Table 77 Node A destination code table, external termination . . . 217
Table 78 Node A destination code table, internal termination . . . 218
Table 79 Node C destination code table, external termination . . . 218
Table 80 Node C destination code table, internal termination . . . 218
Table 81 MCDN feature enhancements . . . 219
Table 82 Module settings for MCDN network . . . 229

Table 83 MCDN dialing plan settings . . . 229
Table 84 Network routing information . . . 230
Table 85 Hardware programming for branch offices . . . 232
Table 86 ETSI network values . . . 233
Table 87 Parts of the NSI string . . . 243
Table 88 Calling numbers required for DPNSS network example . . . 245
Table 89 Routing for DPNSS network . . . 246
Table 90 Default schedule times . . . 251
Table 91 Schedule values . . . 253
Table 92 Schedule values . . . 254
Table 93 Schedule values . . . 255
Table 94 Schedule values . . . 256
Table 95 Ringing and Scheduling Services . . . 257
Table 96 Restriction and Routing Services . . . 257
Table 97 Common settings: Schedule Name . . . 257
Table 98 Common settings: Schedule times . . . 257
Table 99 Set feature values . . . 260
Table 100 Answer keys . . . 262
Table 101 SWCA control values . . . 263
Table 102 System features . . . 264
Table 103 Timer values . . . 265
Table 104 Timer values . . . 266
Table 105 Release reason values . . . 266
Table 106 System speed dial matrix . . . 268
Table 107 Voice message center settings . . . 269
Table 108 ONN blocking settings . . . 270
Table 109 Telco features matrix . . . 271
Table 110 Handset registration and password information . . . 274
Table 111 Radio settings . . . 276
Table 112 Cell information . . . 277
Table 113 Portable telephone programming . . . 279
Table 114 Companion installation information . . . 280
Table 115 Companion installation information . . . 281
Table 116 General and Line access settings . . . 282
Table 117 Capabilities . . . 282
Table 118 User preferences, restrictions and telco features . . . 283
Table 119 Hunt group settings . . . 286
Table 120 Hunt group matrix fields . . . 292
Table 121 Hospitality main settings . . . 295
Table 122 Room settings . . . 296
Table 123 Call permission settings . . . 297
Table 124 Alarm data settings . . . 297

Table 125 Alarm data settings . . . 298
Table 126 Hospitality settings matrix . . . 298
Table 127 DSP resource requirements . . . 302
Table 128 Required MSC resources . . . 307
Table 129 Evaluation of required Business Communications Manager configuration . . . 308
Table 130 Example of required configuration . . . 309
Table 131 Evaluation for the example of required configuration . . . 309
Table 132 MSC information parameters . . . 310
Table 133 MS-PEC information . . . 311
Table 134 Advantages and Disadvantages of Minimum and Maximum values . . . 312
Table 135 MSC configuration parameters . . . 313
Table 136 MSC custom configuration parameters . . . 314
Table 137 MSC component parameters . . . 315
Table 138 Business Communications Manager resources . . . 319
Table 139 LAN global parameters . . . 321
Table 140 Guidelines to configure LAN to LAN traffic smoothing . . . 321
Table 141 LAN attributes . . . 322
Table 142 Additional LAN IP address parameters . . . 324
Table 143 PPP password parameters . . . 328
Table 144 WAN summary parameters . . . 329
Table 145 WAN line parameters . . . 330
Table 146 WAN frame relay parameters . . . 332
Table 147 WAN PVC congestion control parameters . . . 333
Table 148 WAN PPP parameters . . . 335
Table 149 Additional WAN IP addresses . . . 336
Table 150 RAS server TCP/IP parameters . . . 338
Table 151 V.90 modem summary parameters . . . 339
Table 152 Modem link parameters . . . 340
Table 153 V.90 modem access parameters . . . 341
Table 154 ISDN summary settings . . . 342
Table 155 ISDN link parameters . . . 343
Table 156 ISDN access parameters . . . 344
Table 157 ISDN dial-out user parameters . . . 344
Table 158 ISDN channel characteristics . . . 344
Table 159 PPPoE summary settings . . . 347
Table 160 PPPoE link parameters . . . 348
Table 161 PPPoE access parameters . . . 348
Table 162 PPPoE dial-out user parameters . . . 349
Table 163 PPPoE channel characteristics . . . 349
Table 164 Comparing Encryption and Authentication Methods . . . 436
Table 165 Service classes . . . 450
Table 166 Default Queue mapping for Business Communications Manager . . . 453

Table 167 Status page items 463
Table 168 Input Rule Configuration for Unified Manager — RPC 476
Table 169 Input Rule Configuration for Unified Manager — DCOM 477
Table 170 Input Rule Configuration for Unified Manager — port 6800 477
Table 171 Event messages 519
Table 172 Core software, defined by region and carrier profile 575
Table 173 Languages 576
Table 174 South/Central America language breakout 576
Table 175 Companding law 577
Table 176 ISDN line services 578
Table 177 ISDN services, by Protocol 578
Table 178 Mobility services, by region 579
Table 179 Module availability, by profile 580
Table 180 Trunk availability, by region 581
Table 181 PRI line protocol supported, by region 582
Table 182 BRI and PRI line types (DTM and BRI modules) 583
Table 183 Time/date formats based on language 585
Table 184 Region defaults 586
Table 185 Voice Mail default voice mail languages by country 589
Table 186 Feature defaults, by region/country 589
Table 187 Button Programming Feature settings 593

Preface

This guide explains how to program your Business Communications Manager system. For more information about the Business Communications Manager document suite, refer to "Related publications" on page 41.

Note: The section "Software licensing" on page 3 contains software licensing information.

Before you begin

This guide is intended for two main audiences:

- the operator who manages the telephony operations of the system
- the system administrator who manages the data and network operations of the system

This guide assumes the following:

- There is an existing plan outlining the telephony and data requirements for your Business Communications Manager system.
- The Business Communications Manager is installed and initialized and all hardware appears to be working. External lines and terminals and sets are connected to the appropriate media bay modules on the Business Communications Manager.
- That all operators have a working knowledge of the Windows operating system and graphical user interfaces.
- Operators managing the data portion of the system are familiar with network management and applications.

Symbols used in this guide

This guide uses symbols to draw your attention to important information. The following symbols appear in this guide:

Caution: Caution Symbol
Alerts you to conditions where you can damage the equipment.

Danger: Electrical Shock Hazard Symbol
Alerts you to conditions where you can get an electrical shock.

Warning: Warning Symbol
Alerts you to conditions where you can cause the system to fail or work improperly.

Note: Note Symbol
A Note alerts you to important information.

Tip: Tip Symbol
Alerts you to additional information that can help you perform a task.

Text conventions

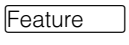
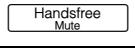
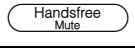
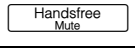
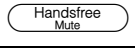
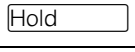
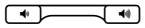
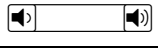
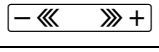
This guide uses the following text conventions:

angle brackets (< >)	Indicates that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **`ping`** *`<ip_address>`*, you enter **`ping 192.32.10.12`**
`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip {alerts|routes}`**.
italic text	Indicates book titles
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
Letters and numbers in boxes (for example: ⎋ 9 8 3)	Indicates the buttons you press on a Norstar telephone.

About the buttons on your telephone

This guide shows the Business Series Terminal buttons. Table 1 shows which buttons to use on the different types of Nortel Networks telephones.

Table 1 Telephone buttons

Button Name	T7100, T7208, T7316	M7100, M7208, M7310, M7324	M7100N, M7208N, M7310N, M7324N
Feature			
Handsfree			
Mute			
Hold			
Volume Control			
Release			

You can enter , or and the code to use a feature. For example: Press 9 8 1 to access your mailbox.

The T7100 terminal works differently from other telephones on your system because it does not have line buttons. Where other telephones can require that you select a line button to answer a call, with the T7100 terminal you pick up the handset. Where other telephones require you to select a line button to take a call off hold, you press on the T7100 terminal.

On T7100 terminals, you can answer a second call by pressing . Your active call is put on hold and you connect to the waiting call. You can have no more than two active calls at one time.

The T7100 terminal does not have a button.

Acronyms

This guide uses the following acronyms:

ANSI	American National Standards Institute
API	Application Program Interface
ARP	Address Resolution Protocol
ASM	Analog station module
ATA (or ATA2)	Analog Terminal Adapter
AUI	Attachment Unit Interface
AWG	American Wire Gauge
BERT	Bit Error Rate Test
BIOS	Basic Input Output System
BKI	Break-in
BLF	Busy Lamp Field
BootP	Bootstrap Protocol
BRI	Basic Rate Interface
CAP	Central Answering Position
CDP	Coordinated Dialing Plan
CHAP	Challenge-Handshake Authentication Protocol
COPS	Common Open Policy Service
COS	Class of Service
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSU	Channel Service Unit
DASS2	Digital Access Signaling System Number 2
DECT	Digital enhanced cordless telecommunications or Digital European cordless telephone
DHCP	Dynamic Host Configuration Protocol.
DiffServ	Differentiated Services
DIMM	Dual In-line Memory Module
DLCI	Data Link Connection Indentifier
DLCMI	Data Link Control Management Interface
DN	Directory Number
DNS	Domain Name Service (DNS)
DPNSS	Digital Private Network Signalling System
DRT	Delayed Ring Transfer

DTMF	Dual Tone Multifrequency.
EDO	Extended Data-Out
FQDN	Fully Qualified Domain Name
HDLC	High-level Data Link Control
HF	Handsfree
HS	Hospitality services
HTTP	Hypertext Transfer Protocol
I/C	Intercom feature button
ICCL	ISDN Call Connection Limitation
IETF	Internet Engineering Task Force.
IP	Internet Protocol
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
IRQ	Interrupt Request
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector (formerly CCITT)
LAN	Local Area Network
LCD	Liquid Crystal Display
MAC	Media Access Control
MAU	Media Access Unit
MCDN	Meridian Client Defined Network (PRI SL-1)
MLPPP	Multi-Link Point-to-Point Protocol
NAT	Network Address Translation
NBMA	Nonbroadcast Multi-Access
NCRI	Network Call Redirection Information
NIC	Network Interface Card
OPX	Off Premises Extension.
OSPF	Open Shortest Path First
PAP	Password Authentication Procedure
PBX	Private Branch Exchange.
PCI	Peripheral Component Interconnect Slot
PPP	Point-to-Point Protocol

PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
QSIG	Q reference point signalling
RAS	Remote access service
RIP	Routing Information Protocol
SAPS	Station Auxiliary Power Supply
SDRAM	Synchronous Dynamic Random Access Memory
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
SPID	Service Profile Identifier
STP	Shielded Twisted Pair
TAPI	Telephony Application Program Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal Equipment
TEI	Terminal Endpoint Identifier
TOS	Type of Service.
TPE	Twisted Pair Ethernet
UDP	User Datagram Protocol
	Universal Dialing Plan
VoIP	Voice over IP
VPN	Virtual Private Networks
WAN	Wide Area Network
WFQ	Weighted Fair Queuing

Related publications

In addition to the *Business Communications Manager Programming Operations Guide*, the Business Communications Manager documentation suite contains the following documents:

- *Business Communications Manager 2.5 Feature Programming Telephone Guide*
- *Business Communications Manager 2.5 Installation and Maintenance Guide*
- *Business Communications Manager 2.5 IP Telephony Configuration Guide*
- *CallPilot Manager Set Up and Operation Guide*
- *CallPilot Reference Guide*
- *CallPilot Quick Reference Guide*
- *CallPilot Programming Record*
- *CallPilot Message Networking Set Up and Operation Guide*
- *CallPilot Message Networking User Guide*
- *CallPilot Unified Messaging Installation Guide*
- *CallPilot Unified Messaging Quick Reference Guide*
- *Business Communications Manager Software Keycode Installation Guide*
- *Nortel Networks Call Center Set Up and Operation Guide*
- *Nortel Networks Call Center Agent Guide*
- *Nortel Networks Call Center Supervisor Guide*
- *Nortel Networks Call Center Reporting Set Up and Operation Guide*
- *Business Communications Manager 2.5 LAN CTE Configuration Guide*
- *Business Communications Manager Personal Call Manager User Guide*
- *Business Communications Manager Attendant Console Set Up and Operation Guide*
- *Business Communications Manager Attendant Console User Guide*
- *Business Communications Manager 2.5 Call Detail Recording System Administrator Manual*
- *Business Communications Manager 2.5 ATA 2 User Guide*
- *CallPilot Fax Set Up and Operation Guide*
- *CallPilot Fax User Guide*

From the Business Communications Manager 2.5 Documentation CD, you can also access a number of telephone and accessory quick reference cards.

How to Get Help

Your local distributor should provide the technical support for your Business Communications Manager system or have access to that information through a Technical Service Center (TSC).

If you require non-technical support, contact 1-800-4NORTEL (1-800-466-7835), choose option 3, Sales or Pre-Sales Support)

Chapter 1
Introduction

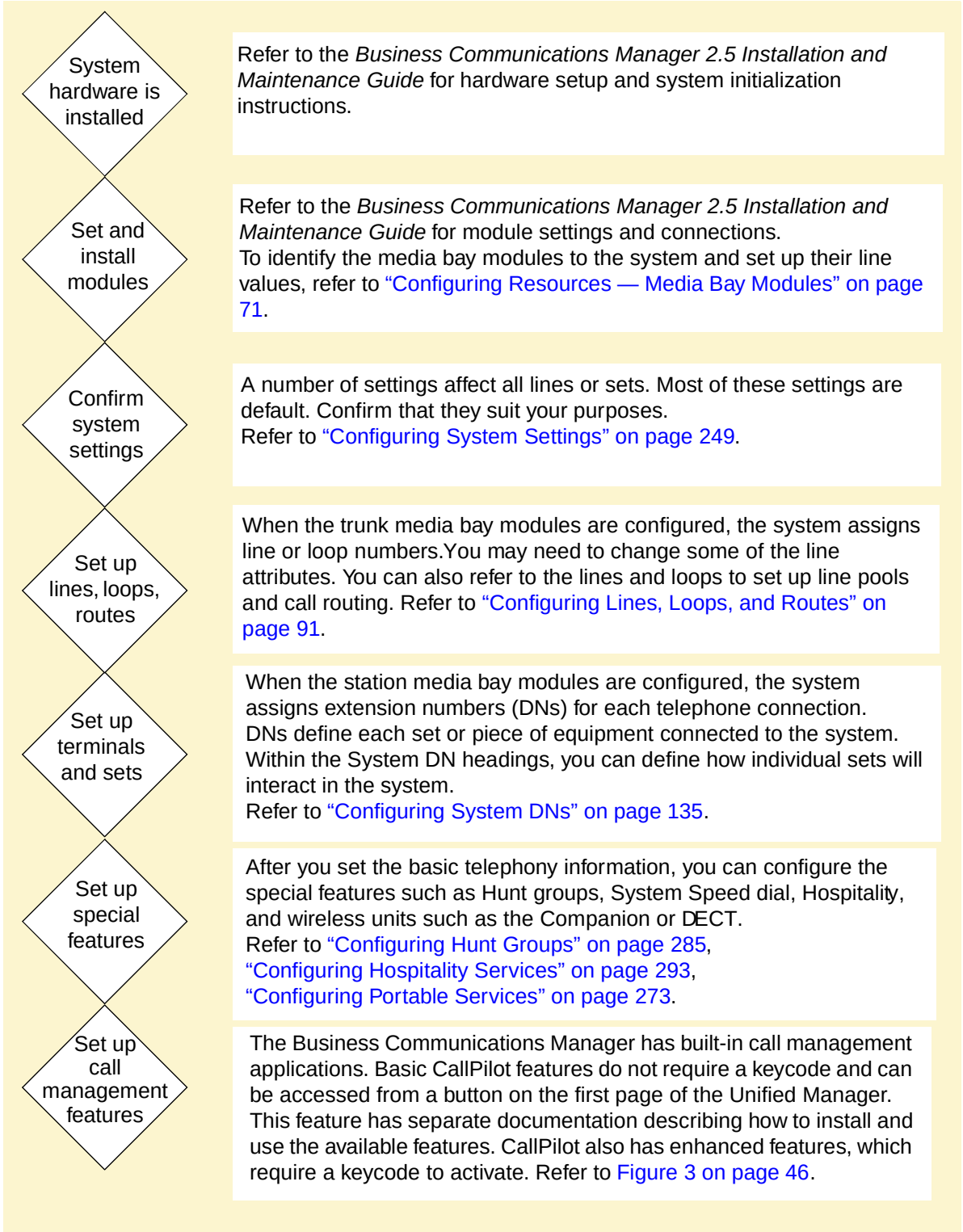
The Business Communications Manager includes software and hardware components that provide telephony, voice messaging, data networking, and IP telephony.

The web-based navigation tool, Unified Manager, provides easy access to all operations and maintenance programming on the Business Communications Manager system at a single site. For more information about Unified Manager, see “Using the Unified Manager” on page 55.

Optivity provides multi-site network management.

Figure 1 on page 44, Figure 2 on page 45, and Figure 3 on page 46 provide an overview of the processes for operating the Business Communications Manager system.

Figure 1 Process for installing the telephony components


System hardware is installed
Refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide* for hardware setup and system initialization instructions.
Set and install modules
Refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide* for module settings and connections.
To identify the media bay modules to the system and set up their line values, refer to "Configuring Resources — Media Bay Modules" on page 71.
Confirm system settings
A number of settings affect all lines or sets. Most of these settings are default. Confirm that they suit your purposes.
Refer to "Configuring System Settings" on page 249.
Set up lines, loops, routes
When the trunk media bay modules are configured, the system assigns line or loop numbers.You may need to change some of the line attributes. You can also refer to the lines and loops to set up line pools and call routing. Refer to "Configuring Lines, Loops, and Routes" on page 91.
Set up terminals and sets
When the station media bay modules are configured, the system assigns extension numbers (DNs) for each telephone connection. DNs define each set or piece of equipment connected to the system. Within the System DN headings, you can define how individual sets will interact in the system.
Refer to "Configuring System DNs" on page 135.
Set up special features
After you set the basic telephony information, you can configure the special features such as Hunt groups, System Speed dial, Hospitality, and wireless units such as the Companion or DECT.
Refer to "Configuring Hunt Groups" on page 285, "Configuring Hospitality Services" on page 293, "Configuring Portable Services" on page 273.
Set up call management features
The Business Communications Manager has built-in call management applications. Basic CallPilot features do not require a keycode and can be accessed from a button on the first page of the Unified Manager. This feature has separate documentation describing how to install and use the available features. CallPilot also has enhanced features, which require a keycode to activate. Refer to Figure 3 on page 46.

Caution: Programming affects system operation.
Only a qualified system administrator should perform startup, installation and maintenance programming. Many of the settings affect correct system operation.

Figure 2 Process for installing the data component

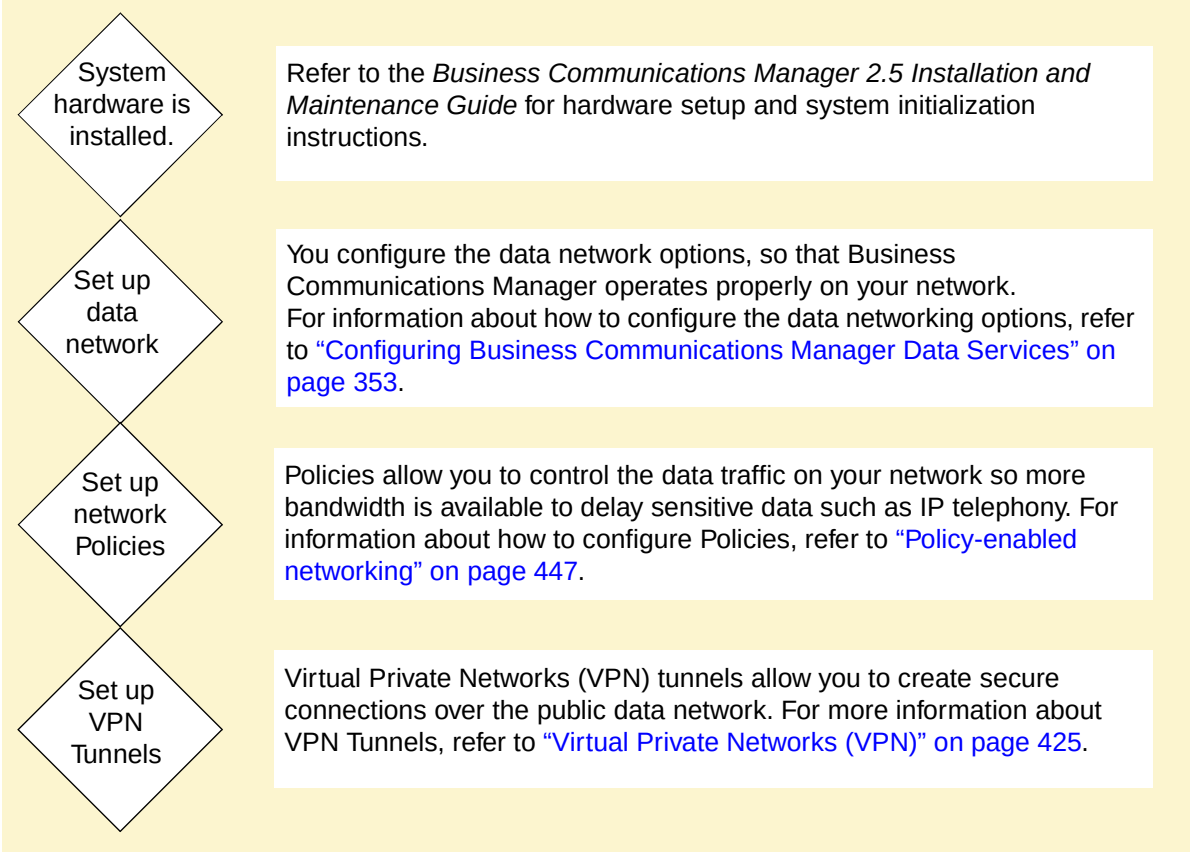
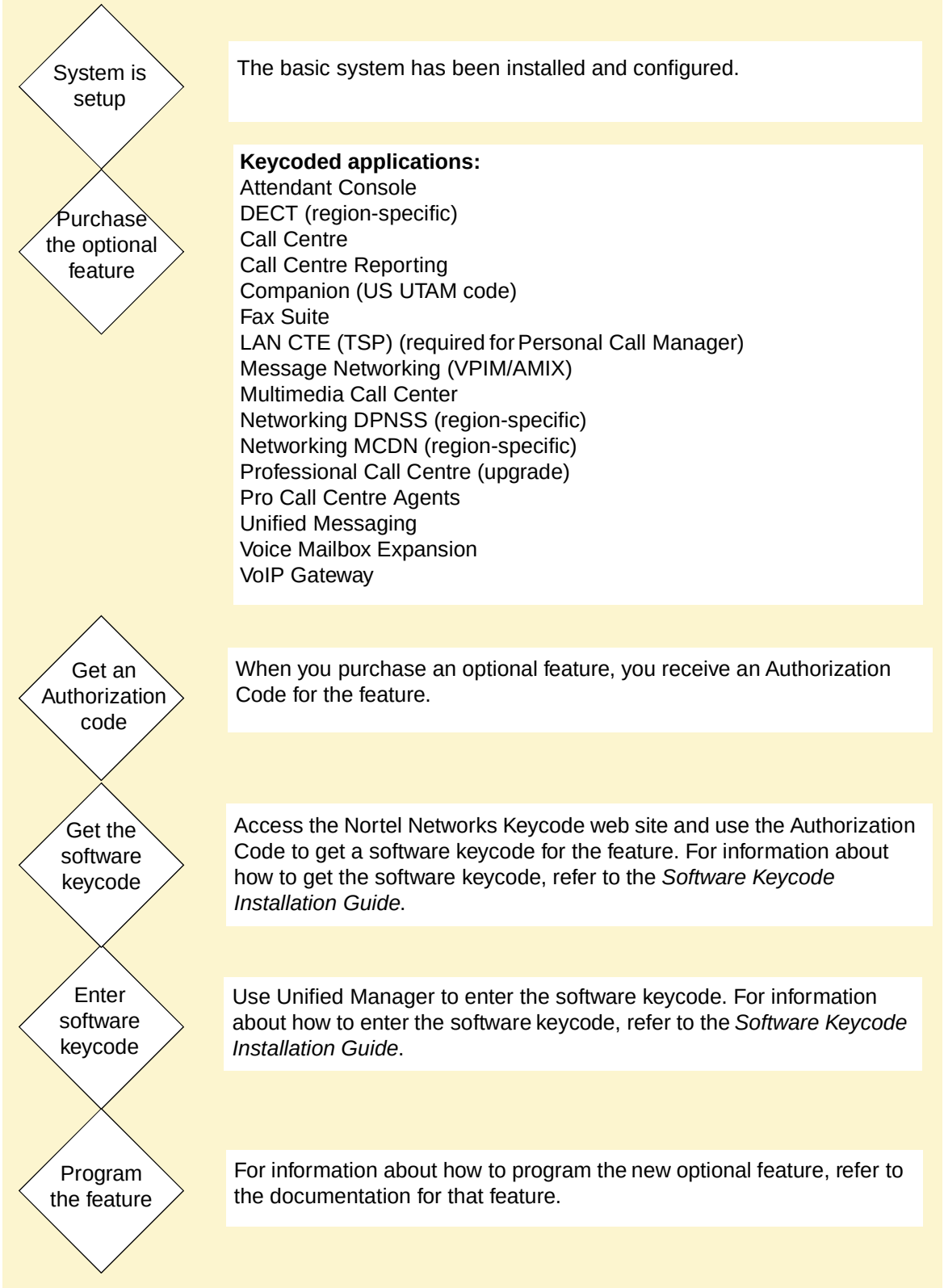

System hardware is installed.
Refer to the Business Communications Manager 2.5 Installation and Maintenance Guide for hardware setup and system initialization instructions.
Set up data network
You configure the data network options, so that Business Communications Manager operates properly on your network. For information about how to configure the data networking options, refer to "Configuring Business Communications Manager Data Services" on page 353.
Set up network Policies
Policies allow you to control the data traffic on your network so more bandwidth is available to delay sensitive data such as IP telephony. For information about how to configure Policies, refer to "Policy-enabled networking" on page 447.
Set up VPN Tunnels
Virtual Private Networks (VPN) tunnels allow you to create secure connections over the public data network. For more information about VPN Tunnels, refer to "Virtual Private Networks (VPN)" on page 425.

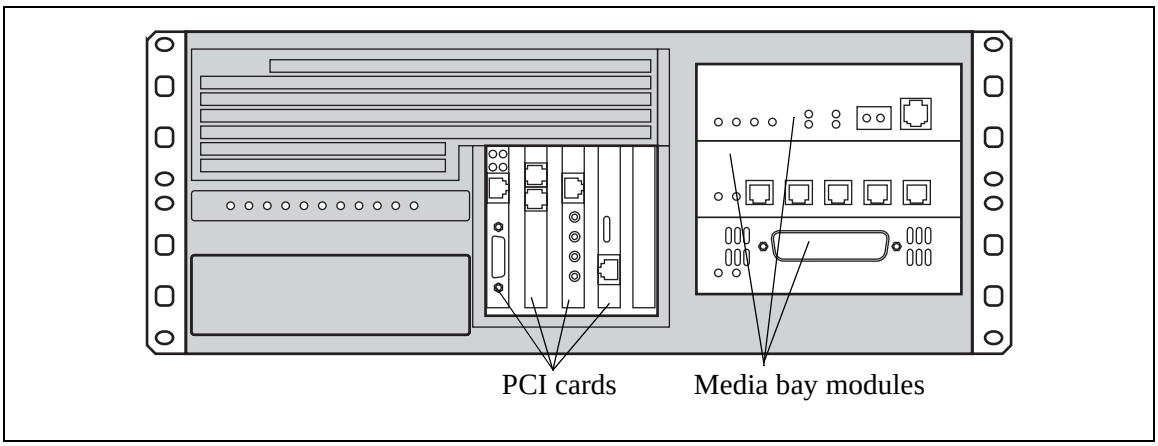
Figure 3 Process for activating optional features


System is setup
The basic system has been installed and configured.
Purchase the optional feature
Keycoded applications:
Attendant Console
DECT (region-specific)
Call Centre
Call Centre Reporting
Companion (US UTAM code)
Fax Suite
LAN CTE (TSP) (required for Personal Call Manager)
Message Networking (VPIM/AMIX)
Multimedia Call Center
Networking DPNSS (region-specific)
Networking MCDN (region-specific)
Professional Call Centre (upgrade)
Pro Call Centre Agents
Unified Messaging
Voice Mailbox Expansion
VoIP Gateway
Get an Authorization code
When you purchase an optional feature, you receive an Authorization Code for the feature.
Get the software keycode
Access the Nortel Networks Keycode web site and use the Authorization Code to get a software keycode for the feature. For information about how to get the software keycode, refer to the Software Keycode Installation Guide.
Enter software keycode
Use Unified Manager to enter the software keycode. For information about how to enter the software keycode, refer to the Software Keycode Installation Guide.
Program the feature
For information about how to program the new optional feature, refer to the documentation for that feature.

System Hardware

The main component of the Business Communications Manager system is the Business Communications Manager server. The Business Communications Manager server controls all tasks such as call processing, voice messaging, and data routing.

Note: Some of the components described in this section are not available in all areas. Ask your Nortel Networks Business Communications Manager supplier for information about the availability of components.



For a detailed description of each hardware component, refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide*.

Business Communications Manager Software

The Business Communications Manager provides a number of software applications. Some applications work immediately after you install the Business Communications Manager system and access the Unified Manager. Refer to Chapter 2, “Getting Started With Unified Manager”, on page 49 for a description of the Unified Manager interface.

To use other applications, you enable the application by entering software keycodes.

Keycodes are based on your system identification and an encrypted code that you obtain when you purchase the rights to an option. Refer to the *Business Communications Manager Software Keycode Installation Guide* for information about how to acquire a keycode and how to enter it. Each of these optional features has separate documentation which includes information keycodes and how to set up the application.

A complete list of options is included in the *Business Communications Manager 2.5 Installation and Maintenance Guide*.

How Does the Network Work?

The Business Communications Manager is designed to run on a LAN and/or aWAN.

For data networking, the Business Communications Manager acts as a policy enabled router that optimizes data traffic and ensures consistent bandwidth for IP telephony,VoIP trunks, and mission critical data.

For telephony applications, the Business Communications Manager base unit acts as a switch and feature controller for the external lines and the internal extensions attached to the sets.

The IP telephone uses both data and telephony features to provide a network-based telephone that provides the call features of the telephony-based digital telephones.

What Do Modules Do?

Media bay modules are key components of the system. They provide the link between the external lines, the Business Communications Manager applications, and the internal extensions, which connect to the telephones.

The type of modules on your system depends on your set requirements and the type of lines available from your service provider. You need to determine this information before you order the system.

Chapter 2
Getting Started With Unified Manager

The Business Communications Manager includes software and hardware components that provide telephony, voice messaging, data networking, and IP telephony.

Unified Manager is the application you use to administer the data, telephony, and maintenance features on the Business Communications Manager base unit.

You access Unified Manager using a web browser. To access Unified Manager you require the IP address of the base unit, as well as a user name and password.

Computer requirements

To run the Unified Manager, you require:

- a 133 MHz Pentium CPU or higher (or compatible)
- 64 MB RAM
- a minimum of 10 MB of available disk space
- a minimum screen resolution of 1024 x 768
- a web browser

Browser Requirements

To use Unified Manager, you require:

- Java Virtual Machine (JVM) 5.0 (build 5.0.0.3188 or greater)
- Netscape Communicator 4.5 or later, or Microsoft Internet Explorer 4.01 or later

If you are using Netscape Communicator, set the following parameters:

- Enable Java: On
- Cached document comparison: Every time

If you are using Microsoft Internet Explorer, set the following parameters:

- Check for newer versions: Every visit to the page
- Java JIT compiler enabled: On

For information about setting these parameters, check the documentation that came with your web browser.

You can access the Business Communications Manager system from another computer through a WAN/Internet connection or a dialup connection. The dialup connection uses either the internal V.90 modem (North America only) or an ISDN dialup. Both access methods create an IP connection that enables all IP-based management tools. For more information on remote connections, refer to "Dial Up" on page 338.

Using a HTTP Proxy server

Unified Manager does not work properly if you use a HTTP Proxy server to connect to the Internet. If you use an HTTP Proxy server, you must change your web browser settings so you can bypass the Proxy Server when connecting to Business Communications Manager.

To Bypass the HTTP Proxy on Microsoft Internet Explorer 5.0

1. On the menu bar, click the **Tools** menu and click **Internet Options**.
2. Click the **Connections** tab and click the **LAN Settings** button.
3. Click the **Advanced** button.
4. In the **Exceptions** box, type the IP address of the Business Communications Manager system.
5. Click the **OK** button until the main browser page appears.

To Bypass the HTTP Proxy on Netscape Communicator 4.5

1. On the menu bar, click the **Edit** menu and click **Preferences**.
2. Click the + symbol beside **Advanced**.
3. Click the **Proxies** heading.
4. Click the **View** button.
5. In the **Exceptions** box, type the IP address of the Business Communications Manager system.
6. Click the **OK** button until the main browser page appears.

Note: If the Business Communications Manager system is located outside of your network, or you have to use a proxy as a gateway proxy to communicate with Business Communications Manager, the procedures above may not work. For these procedure to work, the gateway proxy must be able to understand and pass distributed component object model (DCOM) calls between Business Communications Manager and the computer you are using to run Unified Manager.

Logging on to Unified Manager

Use the following procedure to log on to Business Communications Manager using the web browser:

1. Launch your web browser.
2. In the URL address field, type the Business Communications Manager IP address, including the port number 6800.
   For example: *HTTP://10.10.10.1:6800*

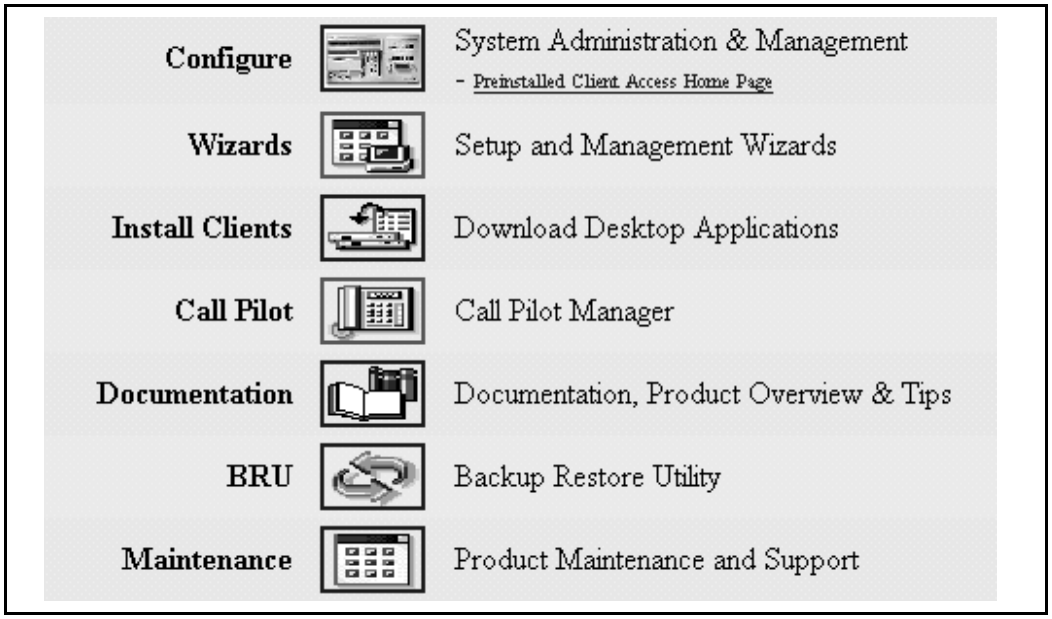
> **Note:** You must include **HTTP://** with the address and port number to access Unified Manager when you are using Internet Explorer as your browser.

The Business Communications Manager Unified Manager initial page appears.

Using the Unified Manager Buttons

On the initial Business Communications Manager Unified Manager web page a number of buttons provide access to various parts of the Unified Manager, including the Unified Manager configuration pages and the configuration Wizards.

Figure 4 Unified Manager first-page buttons



When you first install your system, you must run the Quick Start Wizard to set up your system parameters. This wizard is described in Chapter 3, “Configuring Start-up System Parameters” on page 59.

Once your system is initialized you can access the configuration screens of the Unified Manager using the Configure button. If you choose to preinstall the Java class files, you can use the Preinstalled Client Access Home Page hyperlink for the same purpose. The following two sections describe how to use these two logon methods.

Figure 4 shows the Configure button and the Preinstalled Client Access Page hyperlink.

Using the Configure Button

The Configure Button accesses the Unified Manager programming records for all services except those controlled by the CallPilot service.

1 From the Business Communications Manager main page, Click the **Configure** button.

The Unified Manager login screen appears.

2 In the **Login** box, type your login name.

The default login name is *supervisor.*

3 In the **Password** box, type your password.

The default password is *visor.*

Tips: Ensure that you change the password after you first log on to Business Communications Manager. For information on how to change passwords and to define user profiles, see "User Manager" on page 479.

4 Click the **Login** button.

The Unified Manager software starts. Depending on your system, Unified Manager software can take several minutes to initialize.

5 Refer to "Logging on to Unified Manager" on page 51.

Using the Preinstalled Client Access Home Page hyperlink

You can improve the time it takes to log on to Unified Manager by using the Preinstalled Client Access Home Page. To use this method, you must install the Java class files on your computer first. This method of logging in is faster because you do not have to download the Java class files each time you log on to Unified Manager.

Note: To use dialup maintenance, you must use the Preinstalled Client Home Page to access Unified Manager.

Installing the Java Class Files on Your Computer

To install the Java class files on your computer, follow these steps:

1. Go to the Business Communications Manager Unified Manager first page.

   Refer to "Logging on to Unified Manager" on page 51, if necessary.

2. Click the **Install Client** button.
3. Move to the bottom on the Client Install page.
4. If you are using Microsoft Internet Explorer, click the **Unified Manager Internet Explorer Java Class** link.
   If you are using Netscape Communicator, click the **Unified Manager Netscape Java Class** link.
5. Click the **Run this program from its current location** option.
6. Click the **OK** button.
7. If your browser security is turned on, a SecurityWarning dialog box appears. Click the **Yes** button to allow the install program to run.
8. Click the **Finish** button.
9. Close the browser window.

Note: You install the Java class files on your computer once. You **do not** need to install the Java class files each time you use the Preinstalled Client Access Home Page.

Logging on Using the Preinstalled Client Access Home Page

After you install the Java class files on you computer, you can use the Preinstalled Client Home Page hyperlink instead of the Configure button.

1. Go to the Business Communications Manager first page.

   Refer to "Logging on to Unified Manager" on page 51, if necessary.

2. Click the **Preinstalled Client Access Home Page** hyperlink.
3. In the **Login** box, type your login name.

   The default login name is *supervisor.*

4. In the **Password** box, type your password.

   The default password is *visor.*

   Tips: Ensure that you change the password after you first log on to Business Communications Manager. For information on how to change passwords and to define user profiles, see "User Manager" on page 479.

5. Click the **Login** button.

   The Unified Manager software starts.

Using the Configure Button Features to Manage the System

The screens that appear when you use the Configure button allow you to program your system to suit your data and telephony requirements.

Managing Data Networking on the System

The data networking parameters are accessed using the Service heading on Unified Manager. For information about how to set up the data networking, refer to Chapter 17 to Chapter 19.

Managing the Telephony System

The module information is managed under the Resources menu.

Most of the telephony components are managed through records located under the Services menu.

For information about how to set up the telephony system, refer to Chapter 4 to Chapter 16.

Managing Business Communications Manager Optional Features

After you set up the system and it is operating, you can add the keycodes for any optional features you want to include. Most of these require keycodes.

You access the key-coded applications using the Install Client button.

The program that manages CallPilot is accessed through the Call Pilot button.

For information about how to set up these optional features, refer to the documentation for each application.

Finding Documentation

The entire Business Communications Manager documentation suite, plus a number of training panels are included on your Business Communications Manager computer, as well as on the CD that accompanied your system. Use the Documentation button to find the information you require to help you understand and configure your system to your specifications.

Using BRU

The BRU (Backup and Restore Utility) button, allows you to ensure the integrity of your system data by providing a way to backup your system data and configurations in the way that is most useful for your purposes. Backed up data can be restored to the Business Communications Manager should a system failure occur, such as a prolonged power outage. This book contains a chapter describing this utility.

Maintaining Your System

The Maintenance button accesses a number of maintenance tools that allow you to determine the current status of the various aspects of your Business Communications Manager system. This book contains a section on maintenance, and how to use these tools.

Logging Off the Unified Manager

When you have finished a session on the Unified Manager, you need to log off correctly to protect the integrity of the information you entered.

1. Choose **Business Communications Manager** in the navigation tree.

   The **Logoff** menu is enabled.

2. From the **Logoff** menu, click **Logoff**.

   A message appears that asks you to confirm your request to log off.

3. Click **Yes** to log off.

Using the Unified Manager

Unified Manager provides a web-based navigation tool that allows you to view and change configurations for the Business Communications Manager system.

Most changes made with Unified Manager become part of current Business Communications Manager programming when you select an item from the menu options. However, some changes take effect a minute after the user stops programming. If a programming error occurs, you must reenter the original programming.

Business Communications Manager System Access

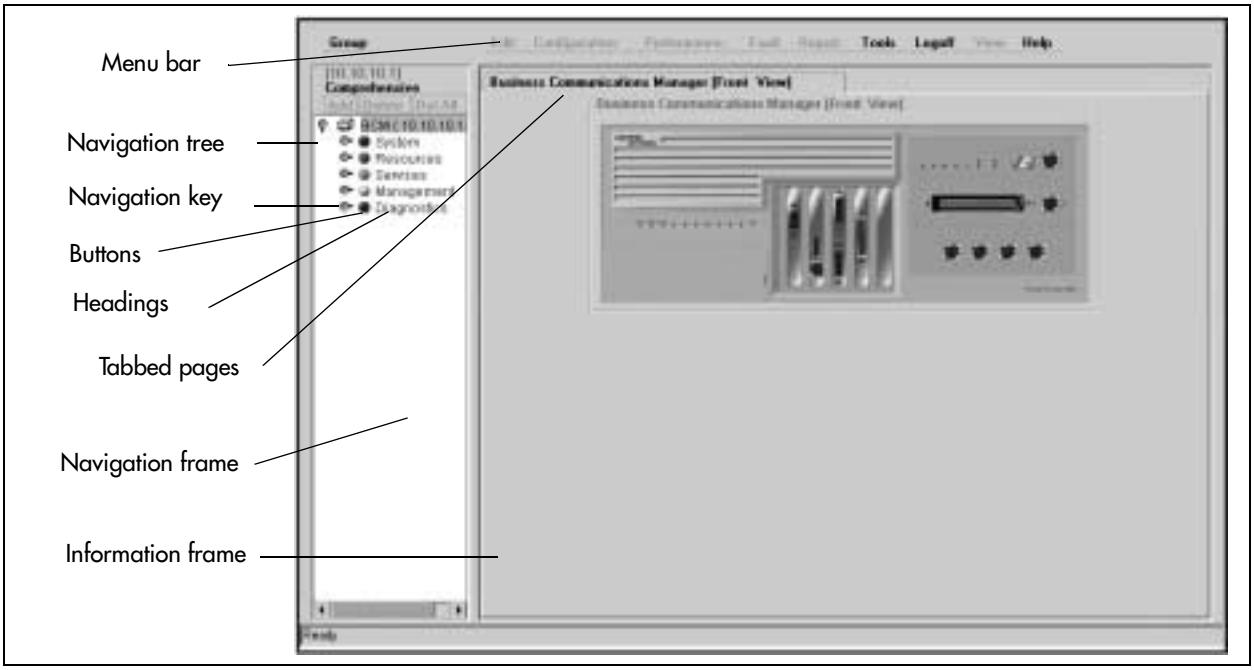
You must control system access by providing one user id, the administrator, with read-write privileges. All other users must be given read-only privileges. This prevents concurrent configuration of the Business Communications Manager system. For information on defining user profile and password, see “User Manager” on page 479.

Unified Manager Display

The Unified Manager screen display, shown in Figure 5, consists of:

- a menu bar where users access configuration commands
- a navigation frame that displays the navigation tree you use to navigate through Business Communications Manager programming headings
- an information frame that displays the windows related to the headings you select in the navigation frame

Figure 5 Main display of the Unified Manager



The menu bar contains configuration management options. When you select the different headings in the navigation tree, these options are enabled. If an option appears dimmed, it is not available for the heading you have selected.

The navigation tree contains headings that allow you to access specific areas of the Business Communications Manager system. The key symbol(⚲) beside each heading indicates that the heading can be expanded to show sub-headings. To display sub-headings, double-click the item or just click on the key itself. As you select various headings in the navigation tree, the heading changes color and Unified Manager displays the appropriate information frame.

Note: If you receive the error message `Telephony programming is currently not available. Please try again later.` when you click on one of the headings, this means that the part of the system that handles MSC is doing a reset. Wait about 1-1/2 minutes and try again.

The information frame can contain configuration windows or dialog boxes indicating the appropriate action or showing system messages or warnings.

Understanding the Dynamic Menu

You access Business Communications Manager functions using the menu bar. The menu bar is dynamic. Commands become active or inactive depending on the heading you select from the navigation tree located in the left frame.

Group	View the system, resources, services, and management.
Edit	Edit parameters.
Configuration	Access configuration dialog boxes and screens.
Performance	Access performance graphs and tables.
Fault	Access fault management settings.
Report	Generate a report.
Tools	Use Business Communications Manager tools.
Logoff	Log off, reboot or shutdown the Business Communications Manager server.
View	Refresh the information window to reflect configuration changes.
Help	Access online help.

Understanding the Navigation Tree Headings

The Unified Manager navigation tree contains five main headings that allow you to access specific areas of the Business Communications Manager system. These headings are described in Table 2.

Table 2 Navigation tree menu functions

Use	To
System	You can expand the navigation tree under the **System** heading to find the **Licensing** and the **Identification** subheadings.
Resources	The subheadings under the **Resources** heading, allow you to configure the following resources: • LAN • WAN • Media Services Card • Media Bay Modules • Dial Up • DECT
Services	Use the options under the **Services** heading to configure services for the Business Communications Manager system, including telephony services.
Management	Use the options under the **Management** heading to configure network management parameters for User Manager and Alarm Manager.
Diagnostics	Use the options under the **Diagnostics** heading to generate and access statistics on different system components. Business Communications Manager provides statistics, metrics and event logs on resources and services to help you carry out system maintenance activities. For more information on using diagnostics tools, refer to Chapter 22, “Maintenance” on page 497.

When you select the **System** heading, you can view system information such as your system name and description and which resources and services are available. Selecting the **System** heading also enabled the following menu options: **Configuration**, **Performance**, **Fault**, **Logoff**, **View** and **Help**. These menu options provide access to statistical information, allow you to enable or disable services and to perform system reboot or shutdown.

For more information on configuring your system settings, refer to "Configuring System Settings" on page 249. For information on Performance and Fault monitoring, refer to "Viewing system performance and fault alarms" on page 535 and "Business Communications Manager system diagnostics and utilities" on page 498.

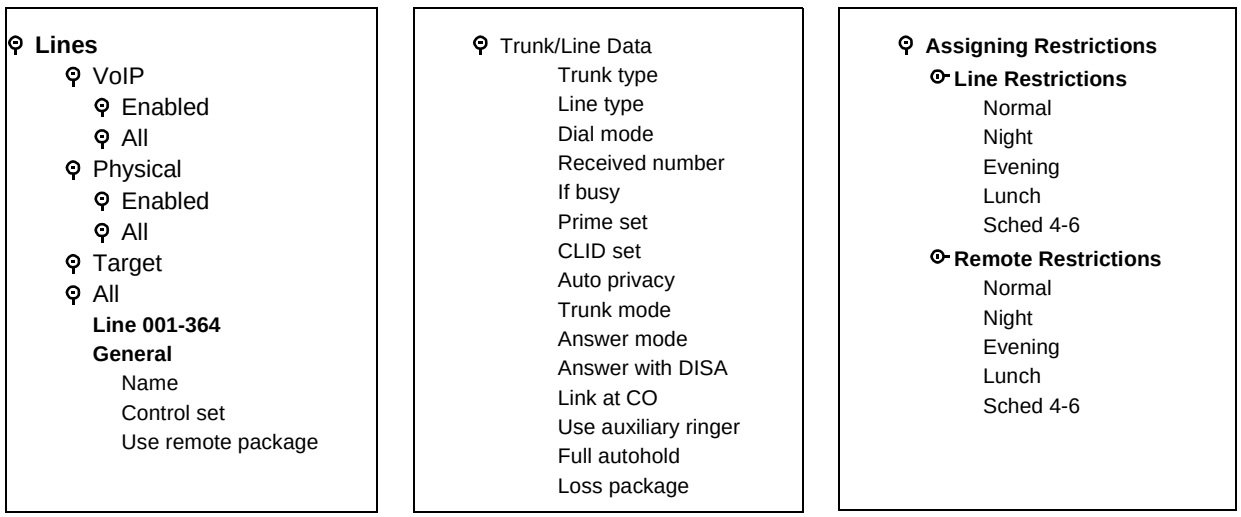
Understanding Tabbed Pages

Some headings display records that have more than one level. Each level is accessed by clicking the appropriate tab at the top of the screen page.

How This Guide Uses the Navigation Tree

At or near the beginning of the major sections of this book, the parts of the navigation tree that are discussed in that section are displayed. A sample of this is shown in Figure 6.

Figure 6 Lines menus and fields



Chapter 3
Configuring Start-up System Parameters

This chapter describes how to configure the basic programming information onto your new Business Communications Manager system using the Quick Start Wizard. This wizard allows you to choose what you want to use as the basic parameters for your system. This includes choosing a system software.

Note: Wizard warnings

Read the Warnings in this chapter before you attempt to use any of the wizards.

Refer to the *Business Communications Manager Installation and Maintenance Guide* for information about installing Business Communications Manager hardware.

Warnings

Read the following Warnings before you attempt to use any of the Wizards.

Warning: Users

Unified Manager allows multiple users to log on to the Business Communications Manager system. If more than one user logs on to configure the same or related subsystems, the most recent modification remains in effect and overwrites changes previously made.

Maintain one user profile with system administrator privileges. If you have more than one system administrator, you must plan configuration changes carefully. Refer to "User Manager" on page 479.

Warning: Running the Quick Start Wizard

Run the Quick Start Wizard only to configure uninitialized systems. When you click the Apply button, Business Communications Manager erases the telephony programming and disables the telephony system temporarily. During application of the Wizard, the Business Communications Manager base unit reboots several times.

Disable the Wizard: To disable the Quick Start Wizard, from the Programming Wizards page click the **Disable Quick Start** link. The Quick Start Wizard icon disappears from the page.

Warning: Wizard timeouts

When the Wizard Instance Timeout Message appears, it indicates that the wizard was inactive for 30 minutes, the wizard has already been applied, or the Business Communications Manager or the server-side wizard component was re-started.

Warning: Do not use Windows NT login sessions while you are using the wizards or while there are wizards being applied.

Accessing the Wizards

The first time you access the **Business Communications Manager - Unified Manager** page, several icons appear.

To access the Wizards:

1. Open up the Unified Manager to the first page of the application.

   Refer to "Logging on to Unified Manager" on page 51 if you need instructions.

2. Click the **Wizards** button.

   The Programming Wizards page appears.

3. In the **Login** box, type your login name.

   The default login name is *supervisor*.

4. In the **Password** box, type your password.

   The default password is *visor*.

5. Click the button for the Quick Start Wizard.

About the Other Wizards

There are other Wizards which you can access from the same page as the Quick Start Wizard. You use these Wizards to program other aspects of the system.

They include the:

- DN Renumber Wizard, which renumbers a range of DNs to a separate range of DNs.
- Edit Template Wizard, which allows you to select one of the five Telephony User Templates and change and define the user settings for individual telephones. The Telephony Template is stored in a file for use with the New User(s) Setup and management Wizard.
- Add Users Wizard, which allows you to change the telephony settings for a range of DNs, or a single DN. You can define the settings in this Wizard, or you can use a pre-defined template created with the Edit Template Setup and Management wizard.

- DECT Configuration Wizard, which allows you to easily configure a DECT module. It also turns on one of the base station ports to allow handset subscription.
- DECT Mobile Recording (handset subscription) Wizard, which allows you to coordinated the cordless handset records between the Business Communications Manager and the DECT module.

The first three wizards described above, are included in Chapter 7, “Configuring System DNs”, on page 135.

The DECT Wizards, which do not appear on the Wizards page if there is no DECT module installed, are described in the *Business Communications Manager 2.5 DECT Installation and Maintenance Guide*.

Navigating the Wizards

This section provides some helpful hints about how the Wizards work, and how to use them.

- To open the online help, from the Programming Wizards screen click the **Programming Wizards Help** link.
- To enable the Quick Start Wizard, from the Programming Wizards screen click the **Enable Quick Start** link. The Quick Start Wizard icon appears on the page.
- You can move back and forth between screens in the Wizards by clicking the **Back** and **Next** buttons.
- You can revise your choices and entries on any of the Wizard pages until you click the **Apply** button. Once you click the Apply button, the system proceeds to apply the selected configurations. The user is presented with a confirmation box that provides the approximate timing of the process. To check the status of the configuration, press the **Refresh** button. When the process is complete, the title of the page has the word *completed* as part of the title.

  The exception to the above is the Edit Template Wizard. On this Wizard, you can go back and forth between the screens, but you cannot change any settings on the first screen once you have moved forward from that page. Therefore, if you need to revise any of the settings, exit the Wizard without clicking the Apply button. Then, start a new Wizard session. Since the Wizard does not retain any information you entered previously, you can pick the same template.

Configuring Your System with the Quick Start Wizard

You can access a Quick Start Wizard from either a serial port connection or a LAN connection. The appearance will be slightly different, but the information required is the same. If you have not already connected your computer to the Business Communications Manager base unit, refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide* for details.

Use the Quick Start Wizard to determine the basic capabilities of your system, such as the name of your system, the CallPilot region (profile), basic data setup, and basic telephony region (profile) and template.

Do not use this wizard until you have read and complied with the warnings printed in "Warnings" on page 59.

Print out or photocopy the next two pages ("What You Need to Know") as a check for the information that you need to know before you run the wizard.

What You Need to Know

Before you start the wizard, ensure you have answers for the following questions:

Screen 1, General information	
• What do you want to call your Business Communications Manager?	(System Name)
• What region do you want to use for the Business Communications Manager CallPilot system? Refer to "Voice Mail Regions" on page 589 for a description of the available choices. If you do not specify a region, the system defaults to North America.	(CallPilot Region)
• What time zone is your system in?	(Time Zone)
Screen 2, Data information (which fields appear will depend on your current data hardware configuration)	
• LAN settings	
IP address	LAN 1: LAN 2:
Subnet mask	LAN 1: LAN 2:
• WAN settings	
IP address	WAN 1: WAN 2:
Subnet mask	WAN 1: WAN 2:
Port (read-only)	WAN 1: T1 WAN 2: V.35
Link Protocol	WAN 1: WAN 2:
• Default Next Hop Router What is the IP address of the next router or link on the network?	(Next Hop on Primary Link)
• DNS What is the domain name of the DNS server?	(IP Domain)
What are the IP addresses (primary and secondary) for the server? Note: Use a space to separate the groups of numbers.	<xxx.xxx.xxx.xxx>
Screen 3,Telephony information	
• What is the mobility protocol your system requires? For more information, refer to "Mobility Services by Region" on page 579.	(Mobility protocol) CT2+ Etiquette DECT

• What is the carrier profile that your system requires? **TIP:** most North American systems use a T1 protocol, while most European-base systems use E1 Refer to "Core Software and Regions" on page 575.	(Carrier protocol) E1 T1
• What is the telephony Region where your system is located? Refer to "Core Software and Regions" on page 575 if you do not know your region.	(Region)
• Software Version (determined by choice of Region)	read-only
• What system template do you want to use for your system?	(Default template) PBX DID
• How many digits will you be using for your system extensions (DNs)? Remember, if your system is part of an MCDN or tandem network, this must be the same length as in all the other nodes if you are using a Uniform Dialing plan.	(Start DN Length)
• What extension (DN) do you want to start at for your sets? Note: the number of digits must agree with the Start DN Length.	(Start DN)
Ignore the following questions if you do not have IP telephones on your system.	
• Are you planning to deploy a large number of IP telephones? The field beside **3/5 DS30 Split to increase IP telephony capacity** determines how many voice channels the Business Communications Manager provides. If you need more information to help you decide, click the **help** link. You can also refer to "Configuring the MSC resources" on page 299.	No = 2/6 split (default) Yes = 3/5 split
• Do you want to be able to immediately start registering Nortel IP terminals on the system?	(Registration) On Off
• Do you want to change the default IP terminal access password?	(Password)
• Do you want the system to automatically assign extension numbers (DNs) to your IP telephones when you install them?	(Auto Assign DNs) On Off

Entering Information in the Quick Start Wizard

This section describes how to use the Wizard to enter the information from the previous section:

1. From the Programming Wizards page, enter the system user name and password, then click on the **Quick Start** button.

   The General page for the Quick Start wizard appears.

2. Enter the required information on the **General** page, **Network** page and **Telephony** page.
3. The **Summary** page contains all the information you entered.
4. Click the **Apply** button.

Chapter 4
Telephony Services Overview

This chapter provides a general overview of the Unified Manager **Telephony Services** headings. This heading is located under the **Services** heading on the navigation tree. The records under this heading allow you to define how the lines and sets in your system will operate.

What lines and what type of sets are available is determined by which media bay modules are active on your system. Refer to Chapter 5, “Configuring Resources — Media Bay Modules”, on page 71, and to the installation charts from the Business Communications Manager 2.5 *Installation and Maintenance Guide*.

Caution: Programming affects system operation.
Only a qualified system administrator should perform startup, installation and maintenance programming. Many of the settings affect correct system operation.

The headings under Telephony Services allow you to program and manage all the voice components associated with Business Communications Manager. You can set up lines and trunks, define settings for individual telephones, and customize your telephone network to suit your requirements.

Figure 7 on page 66 lists the tasks involved in creating the telephony service on the Business Communications Manager system.

Figure 7 Tasks for installing the telephony components

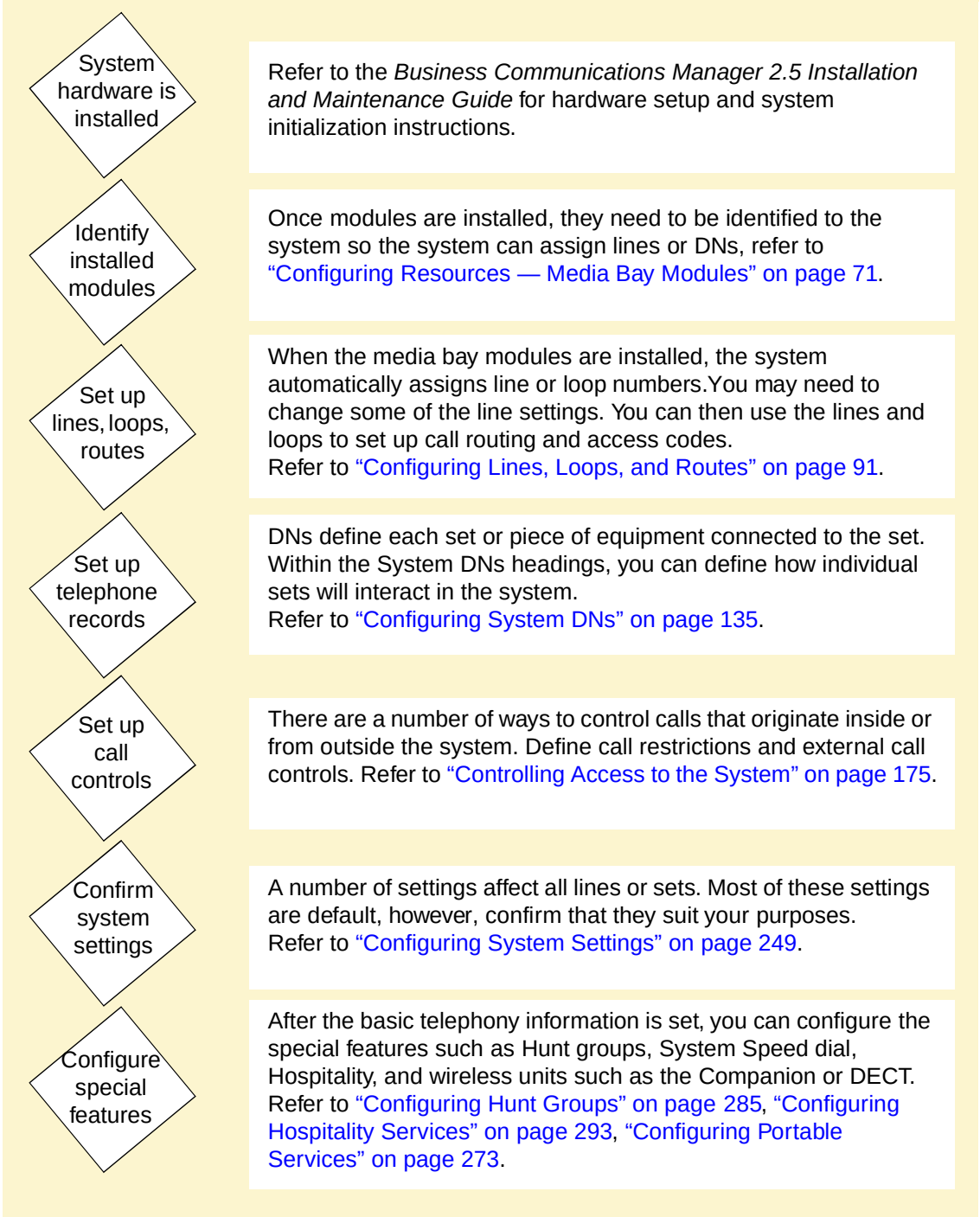

System hardware is installed
Refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide* for hardware setup and system initialization instructions.
Identify installed modules
Once modules are installed, they need to be identified to the system so the system can assign lines or DNs, refer to "Configuring Resources — Media Bay Modules" on page 71.
Set up lines, loops, routes
When the media bay modules are installed, the system automatically assigns line or loop numbers.You may need to change some of the line settings. You can then use the lines and loops to set up call routing and access codes.
Refer to "Configuring Lines, Loops, and Routes" on page 91.
Set up telephone records
DNs define each set or piece of equipment connected to the set. Within the System DNs headings, you can define how individual sets will interact in the system.
Refer to "Configuring System DNs" on page 135.
Set up call controls
There are a number of ways to control calls that originate inside or from outside the system. Define call restrictions and external call controls. Refer to "Controlling Access to the System" on page 175.
Confirm system settings
A number of settings affect all lines or sets. Most of these settings are default, however, confirm that they suit your purposes.
Refer to "Configuring System Settings" on page 249.
Configure special features
After the basic telephony information is set, you can configure the special features such as Hunt groups, System Speed dial, Hospitality, and wireless units such as the Companion or DECT.
Refer to "Configuring Hunt Groups" on page 285, "Configuring Hospitality Services" on page 293, "Configuring Portable Services" on page 273.

Figure 8 shows an overview of the Telephony Services headings in the Unified Manager.

Figure 8 Telephony Services menu options

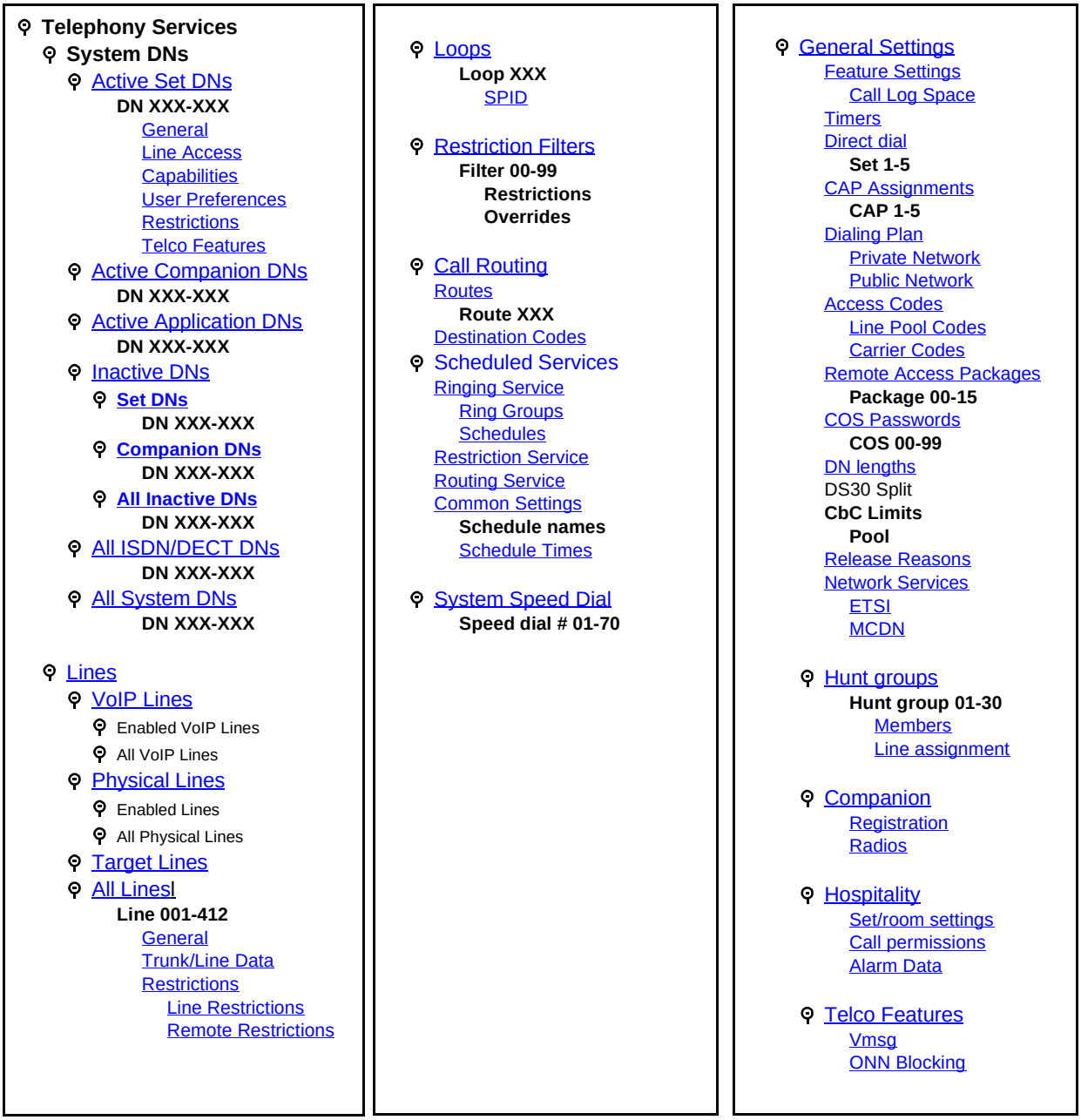


Table 3 summarizes the Telephony Services subheadings. The headings are arranged in the order in which they appear under the Telephony Services heading, not necessarily in the order you would use to program your system.

Table 3 Telephony Services sub headings

System DNs	Allows you to assign settings to each telephone.
Lines	Allows you to assign settings to each trunk and target line.
Loops	Allows you to configure settings for BRI loops.
Defining Restriction Filters	Allows you to apply restriction filters for external calls.
Call Routing	Allows you to define how calls are routed out of your system.
Scheduled Services	Allows you to schedule services, such as night ringing, routing and restrictions.
System Speed Dial	Allows you to create speed dial codes that can be used by any telephone in the system.
General Settings	Allows you to change system-wide settings.
Hunt groups	Allows you to create and manage hunt groups.
Companion	Allows you to assign settings for portable telephones.
Hospitality	Allows you to assign Hospitality settings.
Telco Features	Allows you to assign settings for external voice message services.

Planning

Nortel Networks strongly recommends that you use the planning tables from the *Installation and Maintenance Guide* to understand what lines and set numbers (DNs) are available to you. Coordinate this information with call planning to assess your system requirements. Chart this information to determine how to set up your lines and sets.

DN lengths and the Start DN are identified during initialization of the system. Ensure these settings are correct before you do any other programming. This is especially important if your system is part of a network, where your DN length must match that of the other systems in the network.

Information Matrices

Each section also provides a matrix containing the information from that section. Use this information to create a spreadsheet record of your system configuration:

- “Line Matrix” on page 105
- “Loop Matrix” on page 109
- “Routing Matrix” on page 129
- “Digital Telephones DN Record Matrices” on page 170
- “Direct Dial Matrix” on page 178
- “Target Lines Matrix” on page 179
- “Remote Access Matrix” on page 185
- “Dialing Plans Matrix” on page 183
- “Access Code Matrix” on page 116
- “CbC Matrix” on page 189
- “Restriction Filters Matrix” on page 195
- “Services Matrix” on page 257
- “System Features Matrix” on page 264
- “Timers Matrix” on page 266
- “System Speed Dial Matrix” on page 268
- “Telco Features Matrix” on page 271
- “Hunt Group Matrix” on page 292
- “Hospitality Matrix” on page 298
- “Companion Matrix” on page 280

Networking Systems

If your system is part of a private network, check with the network coordinator for any special routing requirements. Private networking is described in Chapter 10, “Configuring Private Networks”, on page 201.

If you are setting up voice over IP (VoIP) trunks or using IP telephones, the network must be set up correctly both from a Business Communications Manager perspective, and from the type of network the Business Communications Manager is being connected to. Refer to the *IP Telephony Installation and Configuration Guide* for details about setting up either of these features.

Chapter 5
Configuring Resources — Media Bay Modules

This chapter describes the Unified Manager headings that define and control the settings for the media bay modules installed on your system.

Media bay modules provide the Business Communications Manager with physical interfaces to trunk (CO) lines and your system telephones, which are defined by directory number (DNs) records.

Task:

Check settings for the media bay modules installed in the system.

Station modules and Analog station modules:

- Confirm that the DIP switch setting matches the intended Bus (DS30 channel) placement.
- Verify module type and programmed bus type settings under intended Bus # are correct for the type of module installed

Trunk modules:

- Confirm that the DIP switch setting matches the intended Bus (DS30 channel) placement.
- Verify module type and programmed bus type settings under intended Bus # are correct for the type of module installed
- Configure the module parameters of individual modules installed on each Bus #

Note: Data module configuration is described in “Configuring a data module” on page 350.

About the Media Bay Module Records

The **Resources/Media Bay Modules** heading allows you to view and change settings for each media bay module installed in Business Communications Manager.

Note: The *Business Communications Manager 2.5 Installation and Maintenance Guide* provides a comprehensive overview of how to choose media modules, how to set the DIP switches on the modules for the correct DS30 channel and offset, and how to install them into the Business Communications Manager base unit or expansion unit.

The *Business Communications Manager 2.5 Installation and Maintenance Guide* also describes the concept of the 2/6 and 3/5 DS30 channel split, which determines how many channels are available for media bay modules. When to choose to change the DS30 channel split is discussed in the MSC section of this guide. Refer to “Configuring the MSC resources” on page 299.

Term clarification: A DS30 channel is called a Bus on the Unified Manager navigation tree.

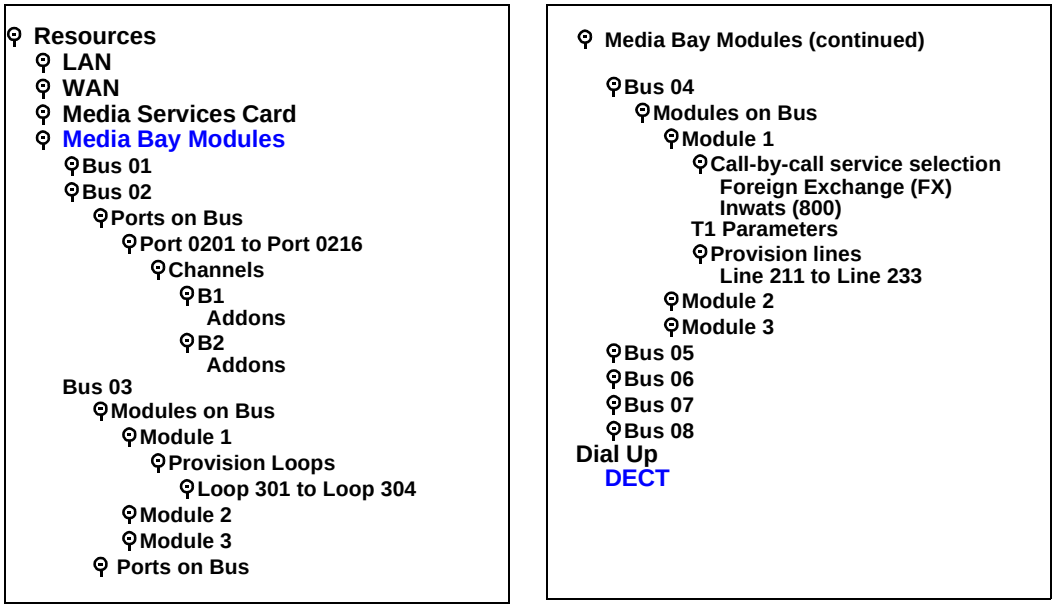
When you choose a region during your system startup, the Business Communications Manager installs a default set of media bay module settings under Resources/Media Bay Modules. However, these may not be the settings that you want for the modules you install. Therefore, when you install a module, you must go to the appropriate Resources/Media Bay Modules/Bus ## record and verify the settings for the module you installed.

Tips: Some modules are region-based and if your system does not have the correct region installed during setup, the modules will not work. Refer to "Media Bay Module Availability by Region" on page 580.

When you configure a media bay module record, the system uses the information in that record to configure the proper range of available lines and/or loops (trunk modules) or system DNs (station modules) that the Business Communications Manager has access to through the module.

Figure 9 illustrates the headings found under **Resources/Media Bay Modules** heading on the navigation tree. The exact items displayed below the Bus number depend on the type of module set with that DS30 channel number.

Figure 9 Resources/Media Bay Modules menus



Media Bay Module Bus Numbers

Under the Bus headings for buses 2 to 7 (or 2 to 6 if your system has a 3/5 DS30 channel split):

- Station or analog station modules display the **Ports on Bus** heading.
- Trunk modules display **Module** plus a number. This number equates to the offsets you set on the DIP switches of the module

Ports on Bus Heading

The MSC presents 16 physical ports for each bus number assigned to a station or analog station module. Each port supports a B1 and a B2 media channel. Digital sets use only the B1 channel on the port, therefore only one set can be assigned to each port. Companion Wireless base stations can use both channels, allowing two handsets to be assigned to each port.

Module # Heading

MSC bus numbers assigned to a trunk module display module numbers which correspond to the offset set on the module DIP switches, as shown in Table 4.

Table 4 Module/Offset correlations

Offset on the module DIP switches	Module # in Unified Manager
0	Module 1
1	Module 2
2	Module 3
3	Module 4

Notes About Media Bay Module Buses

You cannot change headings for buses that are used for internal processing. This section describes how these buses fit into the system.

Bus 1 and Bus 08 provide access to telephony operations for internal processing, applications, and IP sets on the Business Communications Manager system. These two buses are commonly referred to as virtual buses since they have no external physical connections.

Bus 1 has 32 virtual ports. Bus 8 has 28 virtual ports. Each of these ports has one media channel associated with it. These channels are labeled as B1 on the configuration menu.

Bus 08 can also be used for a virtual data module (NA only) when a Business Communications Manager data service such as WAN service is activated. Refer to “Configuring a data module” on page 350 for further programming.

By default, Bus 7 is used for a media bay module connection (2/6 channel split). However, if your system was set to a 3/5 DS30 channel split, then bus 7 becomes a virtual bus with 32 ports. The headings under bus 7 become invalid in this configuration. Refer to the “Configuring the MSC resources” on page 299 MSC programming section for further details.

Configuring Media Bay Modules

After media bay modules are installed into the Business Communications Manager base unit or expansion unit, use the Resources/Media Bay Modules headings to configure the module to the settings that define the lines, loops, or extensions (DNs) that the module will manage.

Dimmed fields are read-only and cannot be changed.

Note: If you receive the error message `Telephony programming is currently not available. Please try again later.` when you click on one of the headings, this means that the part of the system that handles MSC is doing a reset. Wait about 1-1/2 minutes and try again.

Identifying the Module

Use these steps to define a Programmed Bus Type. This setting notifies the Unified Manager about what type of module is installed on the bus (DS30 channel).

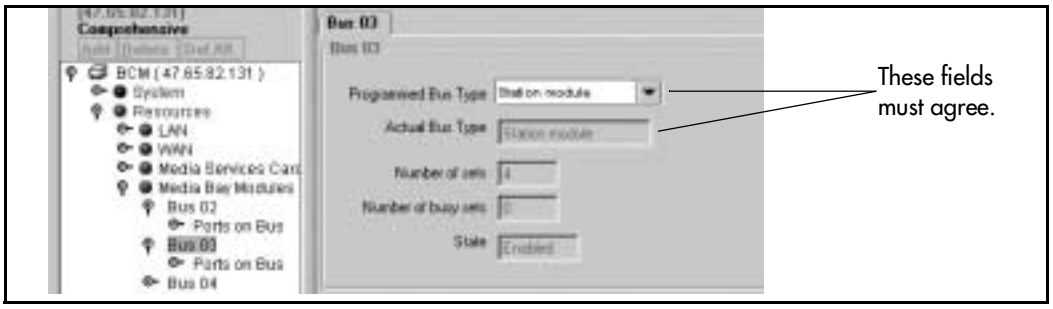
1 Click on the keys beside **Resources**, and **Media Bay Modules**.

2 Click a **Bus** number (Bus 02 to 07).

Refer to Figure 10, which shows the Bus record for a station module.

Tips: Bus number is determined by the DS30 channel set on the DIP switches of the module before it was installed.

Figure 10 Confirming the Programmed Bus Type



3 Ensure the entry in the Programmed Bus Type field agrees with the type of module that is installed for the DS30 channel (bus).

Tips: If the **Actual Bus Type** reads **None**, choose the correct setting in the **Programmed Bus Type** field. After the system initializes to the module, the **Actual Bus Type** should change to the correct module type.

Refer to Table 5 on page 75 for a description of the Bus types available.

Table 5 Programmed Bus Types

Programmed Bus Type	Hardware unit	Capacity	Available line types (some line types are region-dependent) Refer to next section to configure.
Station module	• Digital Station Media Bay Module (DSM 16 or DSM 32)	• DSM16 = 1 bus/16 digital sets • DSM 32 = 2 buses/ 32 digital sets	N/A
	• 4X16 Media Bay Module (4X16) (counts as one DSM 16)	• 4X16 = 1 offset (trunk) and additional bus/ 16 digital sets	
	• Norstar station module (SM) connected to a FEM	• SM = 1 bus/16 digital sets	
Analog station module	• Analog Station Media Bay Module (ASM 8)	• ASM8 = half a bus/8 digital sets	N/A
	• Norstar analog station module (ASM) connected to a FEM	• FEM = 1 bus/16 digital sets	
Trunk module	• Digital Trunk Media Bay Module (DTM)	• DTM = 1 bus/16 lines (max. three DTMs on a system)	• DTMs can be set to module types: Loop, E&M, DID, T1, PRI (NA or ETSI are region-specific)
	• CLID Trunk Media Bay Module (CTM 4 or CTM 8)	• CTM4=1 offset/4 lines • CTM8= half a bus/8 lines	• CTMs can be set to module types: Loop
	• 4X16 Media Bay Module (4X16) (counts as one CTM 8)	• 4X16=1 offset (4 lines) and additional bus (station)	• 4X16s can be set to module types: Loop
	• BRI Media Bay Module (BRI)	• BRI=3 per bus, 4 loops each	• BRI can be set to module types BRI S/T, BRI U2, BRI U4 (setting must match physical module type), U2 and U4 are region-specific
	• DECT Media Bay Module (DECT)	• DECT=1 bus, 4 loops	• DECT (region-specific)
	• Norstar trunk expansion modules, with Analog Trunk cards, connected to a FEM	• FEM=1 bus, can support up to four analog trunk cards (in one trunk expansion unit)/4 lines each	• Norstar analog trunk cards: Loop, E&M, DID
	• Norstar trunk expansion modules with BRI cards, connected to a FEM	• FEM=1 bus, can support up to three BRI cards (in one trunk expansion unit)/4 loops each	• Norstar BRI cards: BRI S/T, BRI U2, BRI U4 (setting must match physical module type). U2 and U4 are region-specific
Data module	Refer to data section of this book for details about setting up a data module on bus 8. For more information, refer to "Configuring a data module" on page 350. This process includes any Norstar Data Modules connected to a FEM.		

4 The other headings on the Bus screen describe the current status of the modules.

Refer to Table 6.

Table 6 Bus XX record settings

Heading	Value	Description
Station module		
Number of sets	<digit>	This setting indicates the number of sets that are currently attached to the module.
Number of busy sets	<digit>	This setting indicates the number of sets that are currently using the module.
State	Enabled Disabled	This setting indicates the state of the module. Use the **Configuration** menu item to change this setting.
Trunk module, Analog Station Module or Data Module		
Number of busy ports	<digit>	This setting indicates how many ports on the module are currently being used.
State	Enabled Disabled	This setting indicates the current state of the module. Use the Configuration menu item to change this setting.

5 Your next steps depend on what type of module you are configuring:

- If you are configuring a station or analog module, ensure that the bus type is correct and the Programmed Bus Type field displays the correct module type. The state field displays Enabled, indicating that the module is active and ready to have telephones connected.
- If you are configuring trunk modules, you must now ensure each module associated with the bus # is set up. This process is described in the next section Defining Trunk Module Types and Settings.

Defining Trunk Module Types and Settings

The Module menu, which appears only under a Bus record that is configured for trunk modules, allows you to configure line or loop provisioning for the module associated with a particular bus.

This record shows the number of lines or loops assigned to the module. It also provides the first and last loop or line number. These settings are read-only.

Trunk lines can also require configuration of settings such as the protocol type/version, frame structure, clocking, and timers. These parameters depend on how the interface of the service provider that the module connects to has been configured.

Note: The fields that appear on the module screen vary depending on the module type you specify.

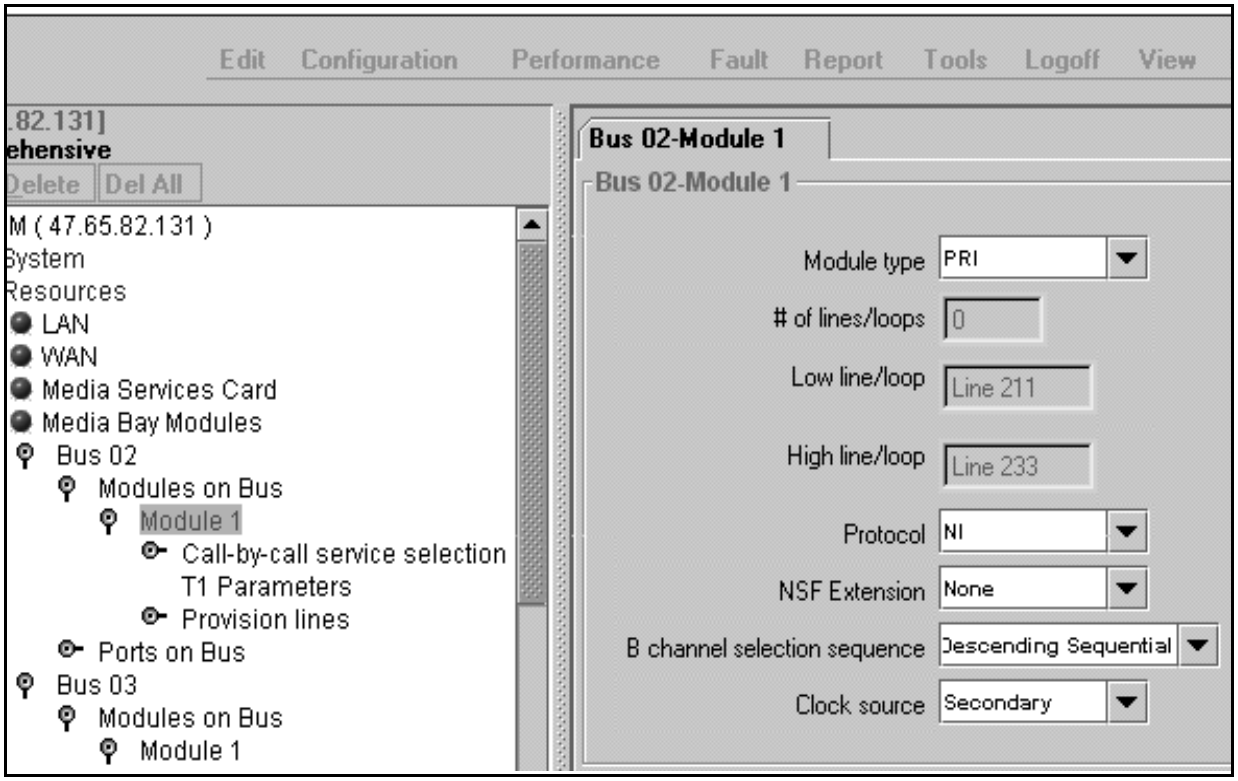
Follow these steps to define the modules to the system:

1 Click on the keys beside **Resources**, **Media Bay Modules**, **Bus <number>**, and **Modules on Bus.**

2 **Click on the Module <number>** you want to program.

The Bus <number>-Module: <number> screen appears. Figure 11 shows an example of the fields that display for a PRI module type.

Figure 11 Example of PRI module settings



3 Click on the arrow beside the **Module type** field and choose the correct setting that defines the type of lines for the module.

The module installed in the system and Module Type must match the defined type of loop or trunk and associated services provided by the central office line that you intend to be connected to the module.

Note: When you configure a media bay module for PRI, BRI, or DECT, the system may download new software to the module. This takes a couple of minutes to complete. Allow the download to finish before continuing to program the module.

4 Press <TAB> on your keyboard to update the record.

Tips: To refresh the record, you may need to click on another navigation tree heading and then re-enter the module record you were working on.

5 Check the settings to ensure they reflect the line requirements.

Refer to Table 7 for a description of each field.

Table 7 Module record values

Module type	Attribute	Value	Description
Loop E&M DID T1 PRI BRI S/T BRI U2 BRI U4	# of lines/loops	<digits>	The total number of lines or loops provided by the loops or trunks on this module.
Loop E&M DID T1 PRI BRI S/T BRI U2 BRI U4	Low/line loop	View only	The lowest line or loop number assigned by the system to the module based on the Bus number, module type, and the module position on the Bus (offset on module DIP switch). Refer to Table 10 on page 84.
Loop E&M DID T1 PRI BRI S/T BRI U2 BRI U4	High/line loop	View only	The highest line or loop number assigned by the system to the module based on the Bus number, module type, and the module position on the Bus (offset on the module DIP switch). Refer to Table 10 on page 84.
Loop T1	Disconnect timer (NA only)	60, 100, 260, 460, or 600 milliseconds	Specify the duration of an Open Switch Interval (OSI) before a call on a supervised external line is considered disconnected. This setting must match the setting for the line at the central office (CO). You must enable disconnect supervision by changing the **Trunk mode** attribute. Under the Telephony Services sub-heading, choose Lines and Line/trunk Data. See "Assigning Trunk/line Data" on page 97 for more information.
E&M T1	Answer timer	1, 2, 3, 4, or 5 seconds	Set the minimum duration of an answer signal before a call is considered to be answered.

Table 7 Module record values

Module type	Attribute	Value	Description
PRI	Protocol	NI-2, DMS100 DMS250 AT&T4ESS SL-1 Euro ETSI Q-Sig	Choose the trunk protocol used by your service provider. The supported protocols are: PRI-T1: NI-2, DMS100, DMS250, AT&T4ESS, SL-1 PRI-E1: ETSI QSIG, Euro, SL-1 Note: SL-1 and ETSI QSIG require MCDN and PRI keycodes to display. BRI: Protocol can also be selected on BRI T-loops under the **Services/Telephony/Loops** heading.
PRI	Protocol type	User Network	When you select SL-1 protocol, an additional setting, Protocol type, appears. Because SL-1 protocol is a private networking protocol, you can designate a Business Communications Manager node as a Network (Master). The default setting is User (Slave). In public network configurations, the CO is generally considered the Network side or Master. Applies to SL-1 protocol only.
PRI	NSF Extension	None WATS ALL	The Network Specific Facilities (NSF) information element is used to request a particular service from the network. Settings are based on the type of switch to which the line connects. Suggested settings: DMS100/250: NONE Siemens ESWD, Lucent 5ESS: WATS GTD5, DMS10: ALL When you select **NONE**, the NSF extension bit is not set for any service. When you select **WATS**, the NSF extension bit is set for unbanded OUTWATS calls. When you select **ALL**, the NSF extension is always set for all CbC services.
PRI	B-channel selection sequence	Ascending Sequential Descending Sequential	Defines how B-channel resources are selected for call processing. For more information, see “Assigning the Number of B channels” on page 108.
T1 PRI BRI-S/T BRI/U2 BRI/U4 DASS2	Clock Source	Primary Secondary Timing Master	Designates whether the DTM/BRI acts as a primary or secondary timing slave or as a Timing Master. Note: A BRI module can be programmed with primary/secondary clock source, however, it is recommended that a BRI module always be Timing Master if a DTM exists on the system to be the Primary clock source. For more information, see “Determining Clock Sources for DTMs or BRIs” on page 80.

Tips: Module type: DECT

The Module Type for the DECT module is DECT. Refer to "Configuring DECT Resources" on page 87 for more information about setting up the DECT module.

6 Press **Tab** to save the settings.

7 If your module is set to T1, PRI, or DASS2, refer to "PRI Call-by-call Service Selection" on page 83 to continue with the configuration.

8 After you have completed your module configurations, refer to Chapter 6, "Configuring Lines, Loops, and Routes," on page 91 to set up the lines the trunk modules will use.

After you have set up your lines and routes, you can set up the extensions (DNs) for the telephones connected to your system. Refer to Chapter 7, "Configuring System DNs," on page 135.

Determining Clock Sources for DTMs or BRIs

Clock Source allows you to designate the DTM or BRI on the system that obtains the timing reference for synchronization from the network.

Systems with digital interfaces need to synchronize to the network in order to function. Synchronization follows a hierarchical path. Each device (switch) obtains the network clock from the device above it in the synchronization hierarchy. The device then passes the network clock to the device below it in the synchronization hierarchy. The synchronization levels are referred to as strata.

Business Communications Manager systems are stratum 4E equipment and are usually used as termination points in a network.

For each DTM and BRI, choose one of the following settings: **Primary**, **Secondary**, or **Timing Master**:

- Primary reference —The DTM/BRI obtains the timing reference from the network and the system synchronizes to it. This is the default value for the first DTM in Business Communications Manager. Note that there should only be one defined Primary clock source on a System.

  Private network: If this system is in a private network and is intended to provide the master clock for that private network, the system must have one and only one Primary clock reference on a DTM or BRI. If this system is intended to act as clock master in a private network, then all clock sources should be set to Timing Master on this system.

- Secondary reference —The DTM/BRI acts as a standby reference. If there are excessive errors on the Primary reference link, or the DTM/BRI designated as Primary reference fails, the Secondary DTM/BRI obtains the timing reference from the network to be used for system synchronization. This is the default value for the second DTM in a Business Communications Manager.

Private network: If this system is in a private network and is intended to provide the Master clock for that private network, then there should be no Secondary reference defined on any DTM/BRI. Note that there should only be one defined Secondary clock source on a system.

- Timing Master —The DTM/BRI does not obtain timing from the network, but transmits the internally-generated system timing, which is derived from the Primary/Secondary source, to equipment connected to it.

  Note that while in the absence of a DTM Primary clocking source a BRI module can be used for the primary timing reference, it is always recommended that, when possible, DTM(s) be used as primary (and secondary) clock sources and that any remaining DTMs/BRIs be set to Timing Master.

Warning: Changing the clock source may disconnect calls.
If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.

Timing Within Networks

In most T1/E1 network configurations, you need one DTM or BRI configured as Primary to act as a primary reference and obtain clocking from the network.

The only application where you might not have a DTM/BRI designated as a primary reference is in a private DTM/BRI network where your Business Communications Manager system is connected to other equipment using T1/E1/BRI interface(s) that require a clock source and your system had been designated as the source of clocking for that private network.

- If the other switches are to be clocked to your Business Communications Manager system, *all* your DTMs/BRIs should be designated as Timing Master.
- If your Business Communications Manager system has two DTMs, you cannot assign both DTMs as primary reference or both DTMs as secondary reference.
  You can have one Primary reference and one Secondary reference per system.
- A T1, PRI(T1), PRI(E1), or BRI can act as the clock source.

T1 Interface Parameters (region-specific)

The T1 Parameters heading appears for module types that have been configured as T1 or PRI. It lets you define a number of settings that are dependent on your T1 service provider settings.

1. Click the keys beside **Resources**, **Media Bay Modules**, **Bus <number>**, **Modules on Bus,** and **Module <number>**.
2. Click on **T1 Parameters**.

3 Configure the T1 parameters according to the information in Table 9:

Table 9 TI parameters

Attribute	Value	Description
CO fail	TIA-547A or TR62411	Select the carrier failure standard used by your T1 or PRI service provider. Consult your T1 or PRI service provider for the proper setting.
Interface levels	ISDN or PSTN	Define a loss plan setting. For more information, see "Interface Levels" on page 82.
Framing	ESF or SF	Select the framing format used by your T1 or PRI service provider: Extended Superframe (ESF) or Superframe (SF). Contact your T1 or PRI service provider for the proper setting. (SF or Superframe is sometimes known as D4.)
Internal CSU	On or Off	Turn the internal T1 channel service unit on or off. For more information, see "Internal CSU" on page 83.
CSU line build	0, 7.5, or 15 dB	Set the gain level of the transmitted signal. This setting appears only when the Internal CSU is set to On.
DSX1 build	000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet	Set the distance between Business Communications Manager and an external channel service unit. This setting only appears when the Internal CSU is set to Off. Contact your service provider for the proper settings.
Line coding	B8ZS or AMI	Define the encoding signals on a T1 line. Select the standard used by your T1 service provider. Contact your T1 service provider for the proper setting.

Interface Levels

The default Interface levels are the ISDN loss plan settings.

Check with your telecommunications service provider to determine if your Business Communications Manager system is connected to a central office (CO) with digital network loss treatment (ISDN I/F levels) or analog network loss treatment (PSTN I/F levels).

The ISDN setting requires digital access lines (DAL) that have digital network loss treatment. On a DAL network, the PBX administers the dB loss not than the CO. DALs may have ISDN signaling or digital signaling (for example, T1). The loss plan follows the Draft TIA-464-C loss plan, which uses a send loudness rating (SLR) of 8 dB. You must contact your service provider to get DAL network loss treatment on a line with digital signaling.

The PSTN setting requires analog access lines (AAL) that have analog network loss treatment and digital signaling. On an AAL(D) network, the CO administers the dB loss.

The loss plan follows the Draft TIA-464-C loss plan. The ISDN loss plan uses a send loudness rating (SLR) of 8 dB and a receive loudness rating (RLR) of 2 dB. The PSTN loss plan uses an SLR of 11 dB and an RLR of -3 dB. If you choose the wrong setting, the voice signal can be too loud or too soft.

Internal CSU

Internal CSU allows you to turn the internal T1 channel service unit on or off. The channel service unit gathers performance statistics for your T1 lines or PRI with public interface. Contact your service provider for the correct settings.

Note: You must disable the DTM before you can change this setting. See "Enabling or Disabling Modules" on page 88 for details.

You can view the performance statistics for your T1 lines in Maintenance under the CSU stats heading. Before you set the internal CSU to off, you must ensure there is an external CSU connected to your T1 lines.

E1 Parameters (region-specific)

The E1 Parameters command appears for modules that have been configured as PRI in an E1 region. There is only one setting in the E1 Parameters menu - the CRC4 setting. CRC4 checking is enabled at the other end.

1. Click on the keys beside **Resources**, **Media Bay Modules**, **Bus <number>**, **Modules on Bus,** and **Module <number>**.
2. Click on **E1 Parameters**.
3. Configure the E1 CRC4 parameter as being On or Off to correspond to the CRC4 setting at the far end of the E1 interface.

PRI Call-by-call Service Selection

This section provides information about how to configure the PRI Call-by-call Service Selection, which is region-specific to North America, for a DTM set a PRI Module type.

By default, incoming calls on a PRI are routed based on the Called Party Number information within the call request. The last number of digits of the called party number which matches the Received Number Length setting, are used as Receive Digits to find a target line.

For example, assume an incoming called party number is 800-555-1234. The received digit number length is 4, and the result is 1234. These last four digits are used to route the call.

In North American PRI, the Call-by-call Service allows alternate routing maps to be defined in various ways, depending on the protocol defined for this PRI.

Use this process to define call-by-call services:

1. Click on the keys beside **Resources**, **Media Bay Modules**, **Bus <number>**, **Modules on Bus,** and **Module <number>**.
2. Click on **Call-by-call service selection**.

Table 10 lists the applicable services for the protocol defined on the Module <number> record.

Table 10 Services available for each PRI protocol

Protocol	Services Available				
	Foreign Exchg	**Inwats (800)**	**Intl-800**	**Switched Digital (SDS)**	**Nine Hundred (900)**
NI-2	SID or All	By number or All	N/A	N/A	N/A
DMS-100	SID or All	SID, By number, or All	N/A	N/A	N/A
DMS-250	SID or All	SID, By number, or All	N/A	N/A	SID, or By number, or All
4ESS	N/A	By number or All	By number or All	By number or All	By number or All

3 Select the service you want to change.

A configuration screen appears in the right frame. The Translation mode default is None.

4 Table 11 shows the possible settings for the services.

Table 11 Module record values

Attribute	Value	Description
Translation Mode	None All By SID By Number	Define how the system maps incoming digits for this service type to the line number within the system. In all cases, the received digits are used to find a target line or to activate Remote Access. **None:** No mapping is applied. The last digits of the Called Party Number which match the Received Number Length setting are used as received digits. Note that if there is no called party number (may occur with some FX calls) the call will ring at the incoming trunk Prime set. **All:** Allows you to define the received digits used for all calls with this service type, regardless of the called party number or service identifier (SID). For this option, all calls with this service type on this PRI will ring the same target line. by SID: Allows you to associate different received digits with different calls of this service type based on the service identifier. **By Number:** Allows you to associate different received digits with different calls of this service type based on party number. NOTE: Any calls that do not match any entry defined in the map table will ring at the prime set. Depending on the service type and the protocol, you may be able to map the called party number (By number) and the service identifier (SID).
Map Table	Select **Add** on the Map Table screen to create a new map entry From *digits* To *digits*	Enter the incoming line number to the internal line number, such as the target line.

Provisioning lines (PRI, T1, & DASS2)

The Provision lines heading allows you to provision and deprovision lines associated with a T1, E1, or BRI ST/U interface.

Provisioning a line or loop makes it available for system use. A deprovisioned line/loop is not available for use.

The line number listed in each **Line <number>** entry corresponds to the line numbers listed under the **Services/Telephony/Lines** menu heading.

Provisioning a PRI or T1 Line

Note that all PRI lines are provisioned by default.

1 Click the keys beside **Resources,** and **Media Bay Modules**.

2 Choose the bus (Bus 02 to 07) associated with the trunk module you want to provision.

Note: Bus 08 is reserved for a data module and has no lines to provision.

3 Click the key beside the **Modules on Bus** heading.

The single DTM module on this bus appear.

4 Choose the module.

5 Expand **Provision lines**.

All the available lines appear as Line <number> headings.

6 Click the line you want to provision.

7 From the Status box, click **Provisioned**.

Provisioning BRI Loops/Lines

In order to provision lines on a BRI module you must first provision the loop on which the lines exist.

1 Click the keys beside **Resources** and **Media Bay Modules**.

2 Click the key beside the bus (Bus 02 to 07) associated with the trunk module you want to provision.

3 Click the key beside **Modules on Bus**.

4 Choose the BRI module where you want to provision loops.

5 Expand **Provision Loops**. All the available loops appear as **Loop <number>** headings.

6 Click the **Loop <number>** you want to provision.

7 In the Status box, click **Provisioned**.

8 After provisioning one or more loops on the module:

a Refresh the **Loop <number>** entry and you will see two **Line *nnn*** entries under this loop.

b Click on the **Line <number>** you wish to provision.

c In the Status box, click **Provisioned**

Deprovisioning a line/loop

When you are not using a line/loop, or when you want to cancel it, you can deprovision that line/loop.

For instance, if your system configuration requires/receives fewer than the standard number of channels delivered from the PRI line, you can deprovision the lines you are not using. This is called Fractional T1/PRI. Your service provider might offer you Fractional T1/PRI service to address specific needs on your system.

You should only have as many lines provisioned on a T1/PRI as you have B-channels being delivered on the T1/PRI from your service provider. Having more lines provisioned and assigned to users may occasionally result in the attempt to perform calls over a line failing because of a lack of B-channel resources being available.

Note: Deprovisioning all of the lines on a DTM does not disable the module.

Note: BRI loops/lines are deprovisioned by default in the N1 ISDN protocol regions, otherwise they are provisioned by default.

Follow these steps to deprovision a line/loop:

1 Click the keys beside **Resources** and **Media Bay Modules**.

2 Click the key beside the bus (Bus 02 to 07) associated with the module you want to provision.

3 Click the key beside **Modules on Bus**.

A list of the modules assigned to the Bus appears.

4 Choose the module you want to provision. For example, click on Module 1.

5 Click the key beside **Provision lines or Provision Loops**.

All the available lines/loops appear.

6 Choose the line/loop you want to deprovision.

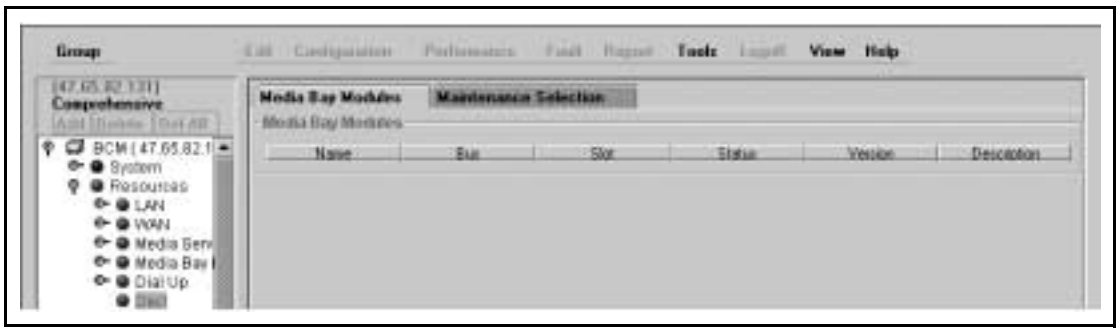
7 From the Status box, click **Deprovisioned**.

Configuring DECT Resources

There are three areas on the Unified Manager that you need to program or look for DECT module information:

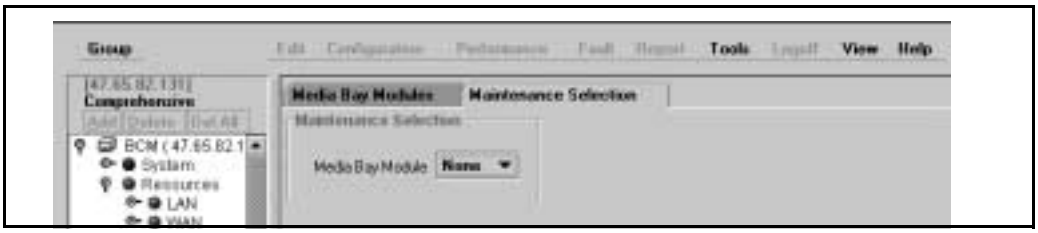
- The DECT module is enabled on the system through the Resources/Media Bay Module/ Bus <number> record, as with all other modules. The difference is that you set the Module Type to DECT.
- The Resources/DECT menu allows you to view the identification information for the DECT media bay module installed in Business Communications Manager. Refer to Figure 12.

Figure 12 DECT Media Bay Module description



- The Maintenance Selection tab opens a screen from which you select the DECT module. This allows you to collect maintenance information that can be viewed through the maintenance console under Services/DECT. Refer to Figure 13.

Figure 13 DECT maintenance selection



The entries on this screen fill automatically when a DECT module is plugged into the Business Communications Manager and the system is powered up. The DIP switch settings on the DECT module define the bus (DS30 channel) and the slot (offset, always set to 0). The information on the module provides the Version and Description information. The status information is obtained from the Provision Lines heading found under Resources/Media Bay Modules/Bus <number>.

The DECT module contains four internally-accessible BRI loops. These loops are also automatically populated when the module is installed.

Note: The module BRI loops are defined within the module to act as a line pool. DNs are assigned to the loops from within the DECT module interface. This also occurs if you configure your system using the DECT wizards. Refer to the *DECT Installation and Maintenance Guide* for details.

DECT Documentation

For detailed information about installing and programming DECT modules, refer to the *DECT Installation and Maintenance Guide.*

Enabling or Disabling Modules

When you are configuring setup information, or troubleshooting the system, you may need to disable a module. The Unified Manager indicates when this is required.

When you disabled a module, lines or telephones (DNs) assigned to that module are disconnected from the system. Enabling the module puts the lines or telephones back in service.

Disabling a Bus

The following procedure describes the process for enabling or disabling a bus. This means that if there is more than one module assigned to the DS30 channel, all modules will be disabled.

1. Click the keys beside **Resources** and **Media Bay Modules**.

   Buses 01 to 08 are displayed.

2. Click on the bus number of the module you wish to enable/disable (Bus 02 to 07).
3. At the top of the screen, click **Configuration**, and then, click **Enable** or **Disable**.
   The system prompts you to confirm your request.
4. Click the **OK** button.

Tips: Remember, if your system has a 3/5 DS30 channel split, Bus 07 will not have a module assigned to it.

Disabling a Single Module

The following procedure describes the process for enabling or disabling a single module if there is more than one module assigned to a DS30 channel.

1. Click the keys beside **Resources** and **Media Bay Modules**.

   Buses 01 to 08 are displayed.

2. Click on the key beside the Bus number of the module you wish to disable (Bus 02 to 07).
3. Click on the Module number of the media bay module you want to enable/disable.
4. At the top of the screen, click **Configuration**, and then, click **Enable** or **Disable**.
   The system prompts you to confirm your request.

5 Click the **OK** button.

Tips: Remember, if your system has a 3/5 DS30 channel split, Bus 07 will not have a module assigned to it.

Chapter 6
Configuring Lines, Loops, and Routes

This chapter describes Lines and Loops. It also describes how to set up your system access codes and how to define routes with destination codes.

Task:

- Understand which lines and loops belong to which trunk modules.
- Program the line and loop settings for the type of lines assigned to the module.
- Create routes for calls to specific lines or using line pools and define destination codes for each route.
- Set up target lines, if required.

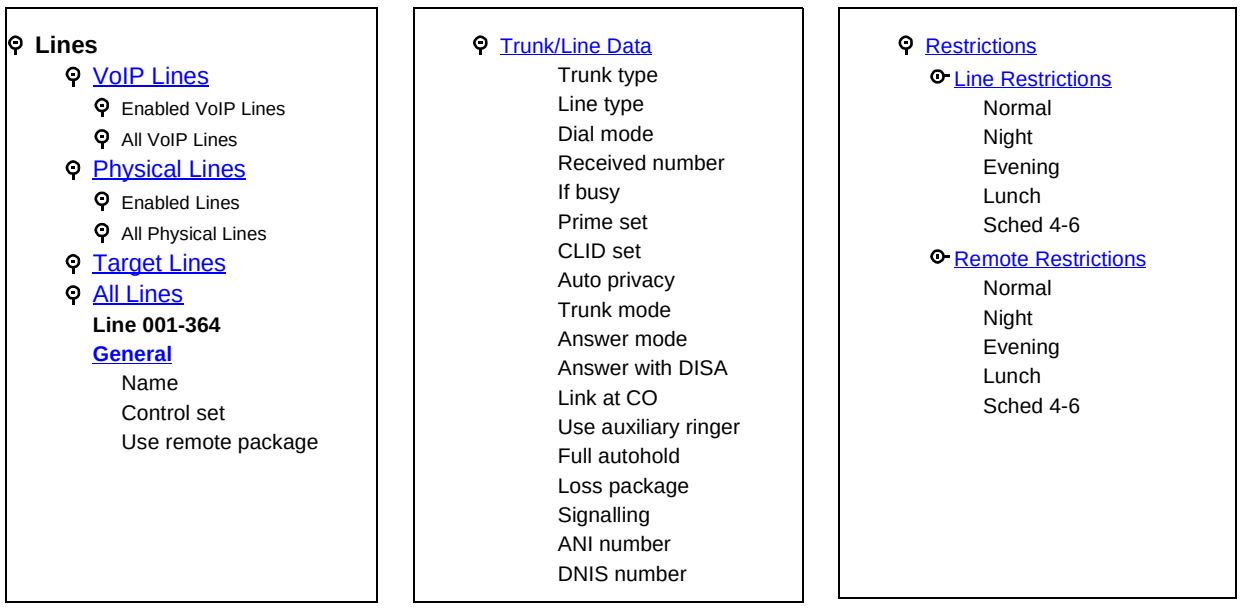
Configuring Line Settings

On a new system, lines and loops are numbered and assigned defaults based on the type of media bay modules that have been connected to the system.

The Unified Manager displays all active physical lines under the **Lines/Physical/Enabled Lines** heading, which allows you to easily to view which lines have been enabled through a media bay module. You can then access each line record and assign attributes, as you require.

Figure 14 shows a detailed view of the Lines navigation tree headings.

Figure 14 Lines menus and fields



Copying Data to Other Lines

The **Copy** command allows you to duplicate programming for a line and apply it to another line or a range of lines.

When you copy data from a physical trunk to a target line (or the other way around), only the data in common is copied. For example, copying a target line to a T1 E&M trunk copies only the Line data settings because there are no Trunk data settings for a target line.

Note: You cannot copy programming between lines on different types of media bay modules. The Received number of a target line is a unique number and cannot be copied.

1. Choose **Services/Telephony Services/Lines/Physical Lines/Enabled Lines**.
2. Click the line number from which you want to copy settings. If necessary, choose a subheading to refine your selection.
3. On the **Edit** menu, click **Copy**.
4. Click **Single** or **Range** from the Copy type list.
5. In the **Copy to** box, type the line number or the start and end line numbers of the range of lines where you want to copy the settings.
6. Click the **OK** button.

Determining Which Lines You Need to Program

Under **Lines**, note that line types are divided into three headings. The fourth heading contains all line numbers, including those which are not assigned to any module.

VoIP Lines

Voice over IP (VoIP) lines are signalling channels that simulate how CO lines work, butVoIP lines transmit data to the IP network over a LAN or WAN rather than over physical lines. Once the VoIP lines are set up, you can assign them to line pools, and program their behavior in the same way you would physical lines.

VoIP lines use line numbers 001 to 060. These line records appear under **Services/Telephony Services/Lines/VoIP Lines**. The number of lines available for use is a function of software key codes.

Note: VoIP trunks do not use line appearances. They must be set up with access or destination codes that the user dials to access the pool of VoIP trunks.

VoIP trunks should be configured to use a single line pool. Do not mix other trunk types on the same line pool. You can use routing to create a fallback capability, where the telephone reroutes the call to another line pool, if the primary route is not available or the call quality is not suitable. If you do not configure your network for fallback and the call quality is below threshold, the IP call will fail.

Refer to the *IP Telephone Installation and Configuration Guide* for details about setting up these lines.

Target Lines

Target lines are internal lines that receive calls and point to specific telephones. You need to set up target lines when you use direct-inward-dial (DID) lines orVoIP trunks. Refer to "Creating Target Lines" on page 178 for instructions about setting up these lines. Systems configured using the DID default template, automatically assign target lines.

Target lines use line numbers 241 to 412. These lines are found under **Services/Telephony Services/Lines/Target Lines**.

Physical Lines

Physical lines are the CO trunk lines connected to the trunk media bay modules. Which lines are enabled is determined by the DIP switch settings on the installed trunk modules. Refer to Table 12 for a list of lines assigned per bus (DS30 channel and offset), based on the module type set with that address.

Table 12 Bus/line-loop default list

Bus #	Type of module	Line/Loop numbers (default) Bus offset 0	1	2	3	Line pool A-O/PRI
		Default start DN: 221				
02	Trunk module					
	DTM (T1)	211-234				
	DTM (NA-PRI)	211-233				
	DTM (E1 PRI)	211-240				
	BRI	211-218	219-226	227-234		
	CTM and **4X16**	211-214	219-222	227-230	235-238	
	CTM8 (upper/lower)	211-214/219-222		219-222/227-230		
		227-230/235-238		235-238/211-214		
	ISDN loops					
	BRI ST/U2/U4	201-204	205-208	209-212		
	DECT	201-204				

Table 12 Bus/line-loop default list

Bus #	Type of module	Line/Loop numbers (default) Bus offset 0	1	2	3	Line pool A-O/PRI
03	Trunk module					
	DTM (T1)	181-204				
	DTM (NA-PRI)	181-203				
	DTM (E1 PRI)	181-210				
	BRI	181-188	189-196	197-204		
	CTM and **4X16**	181-184	189-192	197-200	205-208	
	CTM8 (upper/lower)	181-184/189-192		189-192/197-200		
		197-200/205-208		205-208/181-184		
	ISDN loops					
	BRI ST/U2/U4	301-304	305-308	309-312		
	DECT	301-304				
04	Trunk module					
	DTM (T1)	151-174				
	DTM (NA-PRI)	151-173				
	DTM (E1 PRI)	151-180				
	BRI	181-188	189-196	197-204		
	CTM and **4X16**	151-154	159-162	167-170	175-178	
	CTM8 (upper/lower)	151-154/159-162		159-162/167-170;		
		167-170/175-178		175-178/151-154		
	ISDN loops					
	BRI ST/U2/U4	401-404	405-408	409-412		
	DECT	401-404				
05	Trunk module					
	DTM (T1)	121-144				
	DTM (NA-PRI)	121-143				
	DTM (E1 PRI)	121-150				
	BRI	151-158	159-166	167-174		
	CTM and **4X16**	121-124	129-132	137-140	145-148	
	CTM8 (upper/lower)	121-124/129-132		129-132/137-140;		
		137-140/145-148		145-148/121-124		
	ISDN loops					
	BRI ST/U2/U4	501-504	505-508	509-512		
	DECT	501-504				
06	Trunk module					
	DTM (T1)	91-114				
	DTM (NA-PRI)	91-113				
	DTM (E1 PRI)	91-120				
	BRI	91-98	99-106	107-114		
	CTM and **4X16**	91-94	99-102v107-110115-188			
	CTM8 (upper/lower)	91-94/99-102		99-102/107-110		
		107-110/115-188		115-188/91-94		
	ISDN loops					
	BRI ST/U2/U4	601-604	605-608	609-612		
	DECT	601-604				

Table 12 Bus/line-loop default list

Bus #	Type of module	Line/Loop numbers (default) Bus offset 0	1	2	3	Line pool A-O/PRI
07	Trunk module					
	DTM (T1)	61-84				
	DTM (NA-PRI)	61-83				
	DTM (E1 PRI)	61-90				
	BRI	61-68	69-79	77-84		
	CTM and **4X16**	61-64	69-72	77-80	85-88	
	CTM8 (upper/lower)	61-64/69-72 77-80/85-88	69-72/77-80 85-88/61-64			
	ISDN loops					
	BRI ST/U2/U4	701-704	705-708	709-712		
	DECT	DECT 701-704				

You can change the line types to suit your system. For instance, BRI modules can be designated to a number of line types, depending on the type of line service provided through the central office (CO). However, the line numbers are associated for specific tasks or to specific bus (DS30 channel) numbers.

Use Table 12 to create a quick-view record of the lines and loops available on your system.You can also indicate which pools they are in. Follow these steps to use the table.

1. For each bus number, circle the module you set to that number.
2. Beside the module name, circle the group of line numbers appropriate for the offset you set on the modules.
3. In the Line pool column, indicate a line pool name if you want to associate lines into a pool. This enables assigned telephones to grab any free line from the pool.
4. On the far left column, list the range of DNs you want to associate with each line.

All Lines

This heading contains all possible lines available to the system.

Configuring Line Records

Lines need to be defined and set up, based on how the line will be used.

Under each type of line you will find a record that defines each line. This section explains how to configure each line record.

You can access line records through any of the **Line** headings. The type of line each heading lists is different, but the line records themselves are very similar. Some capabilities are restricted to the line type, but the process for configuring the record is the same.

Using the General Record

The General record allows you to assign the name, a control telephone, and a remote package for a line.

1. Choose the type of line with which you want to work.
2. Under that heading, choose the line number record you want configure.
3. Click **General**.
   Table 13 shows the possible settings for the General record.

Table 13 General record values

Attribute	Value	Description
Name	Up to seven alphanumeric characters	Identify the line in a way that is meaningful to your system, such as by the type of line and line pool or the DN it is attached to in the case of Target lines.
Control set	DN <control telephone DN> Default: 221 (default start DN)	Enter a telephone DN for a telephone that you want to use to turn service off or on for other telephones using this line. The control telephone and the line must be assigned to the same line pool. Refer to "Assigning Line Pool Access" on page 155 **Note:** The start DN is used as the default control telephone for all lines.
	Tips External lines and telephones must be programmed to use one of the Scheduled Services: Ringing, Restriction, and Routing Services. For maximum flexibility, Nortel Networks recommends that you create two different control telephones, one for the lines and one for the telephones. You can turn on a service manually or automatically for all external lines from an assigned control telephone. However, you cannot combine schedules. A service can only be active as normal service or one of the six schedules at any one time. Several schedules can be active at one time, but they must use different services.	
Use remote package	<two digit remote package number>	Package 00: Prohibits remote access to: • line pools • external page This package cannot be changed. Package 01-15 are programmable. Refer to "Remote Access Packages" on page 183

Table 13 General record values

Attribute	Value	Description
	Tips You can program a line pool access code underTelephony Services/General Settings/Access Codes. Refer to "Line Pool Access Codes" on page 114.	

Assigning Trunk/line Data

The **Trunk/line data** heading allows you to program settings for lines that affect how the Business Communications Manager communicates with other switches. These settings also allow you to determine how lines, including target lines, are used in Business Communications Manager.

1 Under the line number you are configuring, click the **Trunk/line data** heading.

Note that the Trunk type field is read-only unless the trunk type is T1.

Note: You can change the trunk type setting only for lines connected to a T1 line. All other lines are automatically configured, based on the type of media bay module present.

Trunk types:

- VoIP
- DTM: TI types (Loop, E&M, DID, Ground, or fixed data channel), PRI, DASS2, DPNSS
- CTM (North America): Loop
- BRI: BRI S/T, BRI U2, U4
- Target lines

BRI note: BRI U2 and BRI U4 are only available through a FEM module connected to a Norstar trunk module with a BRI U2 or BRI U4 card.

2 Configure the line settings according to Table 14. Note that available option fields depend on the line type selected:

Table 14 Line settings table

Trunk types	Attribute	Value	Description
All	Line type	Public Private to: Pool A to O, PRI-A to PRI-F	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O/PRI-A to PRIF: assigns the line to one of the 15 line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. For more information and tips, refer to “Line Pool Tips” on page 101.
Loop start analog Loop start digital Ground start Digital DID E&M	Dial mode	Pulse Tone	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signalling on the trunk. Tone does not appear if Signalling is set to Immediate (T1 DID &T1 E&M trunk types only).
Target lines DASS2	Received #	<digits associated with a specific target line>	Specify the digits to make a specific target line ring. • A received number cannot be the same as, or be the start digits of a line pool access code, a destination code, the DISA DN or the Auto DN. • If you are configuring auto-answer BRI trunks to map to target lines, the received number should be the same as the Network DN supplied by your service provider. The call will be directed to the prime telephone for the incoming line if the Network DN is not used.
Target lines DASS2	If busy	To Prime Busy Tone	Define whether a caller gets a busy tone or the call forwards to the prime telephone when the target line is busy. Busy tone only works for PRI trunks.
All	Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
All	Distinct ring in use	read-only	This field shows the Distinct Ring Patterns that have already been assigned to at least one line.

Table 14 Line settings table (Continued)

Trunk types	Attribute	Value	Description
All	Distinct ring	None, Pattern 2, Pattern 3, Pattern 4	Choose the distinctive ring pattern that you want to assign to the telephone. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority will ring first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None
			Warning: If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. If you assign a distincitive ring pattern to a telephone, and that distincitve ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None. Refer to “Distinct rings in use” on page 162.
Loop start analog Loop start digital E&M digital BRI Target lines DASS2 DPNSS	CLID set	DN: None	Specify which telephones are capable of using the Call Line Identifier (CLID) feature.
Loop start analog Loop start digital Ground start Digital DID E&M BRI VoIP	Auto privacy	Y or N	Define whether one Business Communications Manager user can select a line in use at another telephone to join an existing call.
			Tip: Users can change the privacy setting for the line for an individual call using the Privacy feature (8 3).
Loop start analog Loop start digital	Trunk mode	Unspr Supervised	Define whether disconnect supervision, also referred to as loop supervision, releases an external line when an open switch interval (OSI) is detected during a call on that line. You must set this to Supervised if a loop trunk has its Answer mode set to Auto or if you enable Answer with DISA. Disconnect supervision is also required to conference two external callers. The line must be equipped with disconnect supervision from the central office for the Supervised option to work.
			Tips: The duration of an open switch interval (OSI) before Business Communications Manager disconnects a call is programmed by the **Disconnect timer** setting.

Table 14 Line settings table (Continued)

Trunk types	Attribute	Value	Description
Loop start analog Loop start digital Ground start Digital E&M BRI DPNSS	Answer mode	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer trunks are used to allow external callers to access the system. The system answers with a straight dial tone if DISA has not been enabled. It answers with a stuttered dial tone if DISA is enabled and the caller is expected to enter a COS password.
			Note: You require Disconnect supervision on the line if loop start trunks are to operate in auto-answer mode.
Loop start analog Loop start digital Ground start Digital E&M BRI	Answer with DISA	Y or N	Define whether the system prompts a caller for a six-digit class of service (COS) password. This setting appears for T1 loop start and T1 E&M lines that have auto-answer mode. Set this option to No for T1 E&M lines on a private network that have auto-answer mode. To program DISA on a PRI trunk, see "Creating Direct Inward System Access (DISA)" on page 180.
Loop start analog	Link at CO	Y or N	Some exchanges respond to a Link signal (↻ 7 1) by providing an alternative line for making outgoing calls. When you enable Link at CO, the system applies the restrictions on outgoing calls to the digits dialed after the Link signal, and the call on the alternative line is subject to all restrictions. Disabling Link at CO prevents a Link signal from resetting the Business Communications Manager restrictions in cases where the host exchange does not provide an alternative line.
Loop start analog Loop start digital Ground start Digital DID E&M BRI Target lines VoIP DASS2 DPNSS	Use auxiliary ringer	Y or N	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
			Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to "Ringing Service" on page 253
Loop start analog Loop start digital BRI VoIP DPNSS	Full autohold	Y or N	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. Applies to loop start and VoIP trunks. Full autohold is always in place for T1 E&M trunks; it has no meaning for incoming-only T1 DID trunks. The default setting should be changed only if Full autohold is required for a specific application.
Loop start analog	Loss Packages	Short CO Medium CO Long CO Short PBX Long PBX	Allows you to select the appropriate loss/gain and impedance settings for each line. For more information refer to "Using Loss Packages" on page 102.

Table 14 Line settings table (Continued)

Trunk types	Attribute	Value	Description
DID E&M	Signalling	WinkStart Immediate DelayDial	Defines the signal type for the line. Applies to T1 E&M or T1 DID trunks. The immediate setting does not appear for T1 E&M or T1 DID trunks connected to a DTM if the Dial mode is set to tone. Make sure that this matches the signal type programmed for the trunk at the other switch.
DID E&M	ANI Number	Y or N	Defines whether the telephone number of the caller will be collected for this line. Applies to T1 E&M and T1 DID trunks. For T1 E&M and T1 DID trunks connected to a DTM, this setting only appears if Signalling is set to WinkStart. The central office must deliver ANI/DNIS in DTMF mode. No additional equipment is required.
E&M	DNIS Number	Y or N	Defines whether the digits dialed by an external caller on this line will be collected. Applies to T1 E&M trunks. For T1 E&M trunks connected to a DTM, this setting only appears if Signalling is set to WinkStart and Answer mode is set to Manual. These digits are required for some third-party software applications.

Warning: Enable modules

If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.

Received #

Target lines provide one additional record under **Trunk/Line Data**, and that is the **Received number**. This is the extension number of the telephone that the target line is tied to.

1 Click on **Received Number**.

The Line XXX Received Number screen appears.

2 Enter the DN of the telephone assigned to receive incoming calls which use this line.

Line Pool Tips

Read these tips before you assign your line pools.

- Line pools must never contain a mixture of lines. All lines in a given line pool should go to the same location.
- Avoid putting unsupervised loop start lines in a line pool. These lines can become unuseable, especially when a remote user uses the line pool to make an external call.
- You must assign line pool access to telephones in **Line access** programming.
- You must assign system-wide line pool access codes in **General settings** (not applicable to PRI pools).

Using Loss Packages

The **Loss package** settings allow you to select the appropriate loss/gain and impedance settings for each line. The setting is based on the terminating switch type and the distance between Business Communications Manager and the terminating switch.

When measuring the distance from Business Communications Manager to CO and from Business Communications Manager to PBX, use 600 ohms as the termination resistance setting.

Loss Package	Receive Loss	Transmit Loss	Impedance	Distance to switch/cable loss/terminating switch
Short CO	0 dB	3 dB	Short	Short/<2 dB/Business Communications Manager to CO
Medium CO	0 dB	0 dB	TIA/EIA 464	Medium/>2 dB and <6 dB/Business Communications Manager to CO
Long CO	-3 dB	0 dB	TIA/EIA 464	Long/>6 dB/Business Communications Manager to CO
Short PBX	0 dB	0 dB	Short	Short/<2 dB/Business Communications Manager to PBX
Long PBX	-3 dB	0 dB	TIA/EIA 464	Long/>2 dB/Business Communications Manager to PBX

A loss of 4 dB corresponds to a cable length of approximately 2700 m (9000 ft).

If you are configuring auto-answer BRI trunks to map to target lines, the received number should be the same as the Network DN supplied by your service provider. If the Network DN is not used, the call is directed to the prime telephone for the incoming line.

Tips

A telephone can be administered to search automatically for an idle line from several lines that appear on the telephone. Assign a line pool as the prime line (in **Line access**) and all the lines in the line pool must appear on that telephone. When the user lifts the receiver or presses Handsfree/Mute, any one of the lines, if idle, can be selected by Automatic Outgoing Line selection.

Changes in the settings for trunk type on a system that is in use, can result in dropped calls.

When assigning lines to line pools, consider your network configuration. You can create a unified dialing plan by assigning lines to the same location to the same line pool on each of your systems. For example, if system A and system B each have tie lines to system C, assign the tie lines to pool D on each of the systems.

You cannot assign target lines to a line pool.

Assigning Restrictions

Restrictions prevent you from making certain kinds of calls from specific lines on the telephone. You can also restrict some features. This section describes how to apply restriction filters to lines.

Note: The default template has a set of default restrictions in Restriction 02, only.You must create your own restriction files if you want to use other settings. For details about creating restriction files, refer to "Defining Restriction Filters" on page 190

Line Restrictions

The Line restrictions attribute allows you to specify the filter applied to this line to restrict the dial-out numbers. You can assign a different restriction filter for normal service and for each of six schedules.

Refer to "Scheduled Services Headings" on page 249 for more information about setting up schedules. For PRI, line restriction changes apply to all 23 lines.

Follow these steps to create line restrictions:

1. Choose **Services**, **Telephony Services**, **Lines**, **Line nnn**, **Restrictions**,
2. Click on the key beside **Line restrictions**.
3. Click the schedule heading that you want to configure.

   For example, **Night**.

   The Line restriction window for that schedule appears.
4. In the **Use filter** box, type in the number of the restriction filter you want to assign as the line restriction for this schedule.

   The default restriction filters are listed in Table 15.

Table 15 Default restriction filters

Schedule	Restriction filter
Normal	03
Schedule 1 (Night)	21
Schedule 2 (Evening)	22
Schedule 3 (Lunch)	23
Schedule 4	00
Schedule 5	00
Schedule 6	00

Tips: When a remote user places an external call on a line, any filters used with the line still apply.

Remote Restrictions

Specify the restriction filter for the line that remote callers use to call in to Business Communications Manager. As with line restrictions, you can apply a different remote restriction for normal service and for each of the six schedules.

Follow these steps to set up remote restrictions.

1. From the **Lines** headings, choose the line you want to set restrictions for.
2. Click on the key beside **Remote restrictions**.
3. Click the schedule heading that you want to configure. For example, **Night**.

   The Remote restriction window for that schedule appears.
4. In the **Use filter** box, type in the number of the restriction filter you want to assign as the remote restriction for this schedule.
5. Select the remote restrictions for each schedule. The default restrictions are shown in Table 16.

Table 16 Default remote restrictions

Schedule	Restriction filter
Normal	04
Schedule 1 (Night)	31
Schedule 2 (Evening)	32
Schedule 3 (Lunch)	33
Schedule 4	00
Schedule 5	00
Schedule 6	00

Tips: The remote restriction restricts the numbers a user can dial on an incoming auto-answer line. If a remote user then selects a line to place an external call, any filter used with the line still applies.

Telco Features

If you subscribe to a voice message service outside your office, you can access it through your Business Communications Manager system. You can specify what voice message center you use for each external line that receives message waiting indication.

1. Choose **Services**, **Telephony Services**, **Lines**, **Line nnn**.
2. Click the **Telco features** heading.

   The Telco features window for the line appears.

3 Select the Voice message center for the line, **Center 1** - **Center 5** or **None**.

Note: To program the external numbers for each Center, refer to "Voice Message Center Numbers" on page 269.

Line Matrix

To help you with your line planning, transfer the following information to a spreadsheet and fill out the values for each line you provision.

Table 17 Line attributes

General			
Name			
Control set			
Use remote package			
Trunk/line Data			
Trunk Type			
Line Type		Answer with DISA	
Dial mode		Link at CO	
Received #		Use auxiliary ringer	
If busy		Full autohold	
Prime set		Loss package	
CLID set		Signalling	
Auto privacy		ANI Number	
Trunk mode		DNIS Number	
Answer mode			
Line restrictions		**Remote restrictions**	
Normal	03	Normal	04
Schedule 1 (Night)	21	Schedule 1 (Night)	31
Schedule 2 (Evening)	22	Schedule 2 (Evening)	32
Schedule 3 (Lunch)	23	Schedule 3 (Lunch)	33
Schedule 4	00	Schedule 4	00
Schedule 5	00	Schedule 5	00
Schedule 6	00	Schedule 6	00

Configuring Loops

The **Loops** headings allow you to program BRI S/T, U2, and U4 loop settings.

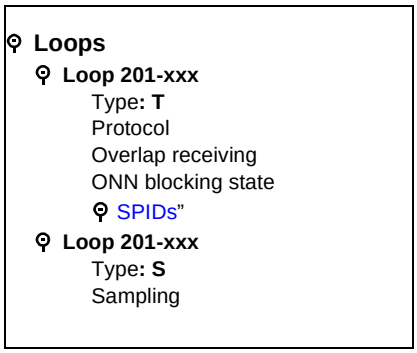
The DECT module also uses BRI loops.

Task:

- Understand which loops belong to which trunk modules.
- Program the loop settings for the type of lines assigned to the module.

Figure 15 shows a detailed view of the Loops commands

Figure 15 Loops headings.



Note: Some headings vary according to the region defined on your system.

Configuring the Loop Type

The Media Bay Modules support BRI ST, U2, and U4 ISDN loops.

Loops are assigned based on your choices under the **Module #** under the **Resources/Media Bay Modules** heading. The system assigns loop numbers once the BRI module is identified to the system. The assigned numbers are based on the module number and offset used on the module.

Follow these steps to configure a loop type:

1. Choose **Services**, **Telephony Services**, **Loops**.
2. Click on the loop number you want to configure.
3. Configure the loop settings according to Table 18:

Table 18 Loop settings

Attribute	Value	Description
Which fields appear depends on the loop type.		
Protocol	Euro, Q-Sig, NI	Select the appropriate ISDN protocol. The values displayed depend on both the market profile and software keycodes. NI - National ISDN Euro - ETSI ISDN standard Q-Sig - also an ETSI standard. Only appears if the ETSI Q-Sig keycode is loaded.
Overlap receiving	Y or N	Supports target lines in markets which use Overlap receiving signalling on the BRI trunks. Overlap receiving must be configured for each BRI loop.
Local number length	0-10	Set the local number length for loops to interfaces that receive overlap rather than enbloc digits. This number is the total length of the called party number received. This number is used to calculate the number of leading digits that need to be removed by the system.
		Note: This parameter appears only when Overlap receiving is set to Y. Example: Public received number = 4502303 Target line received numbers = 303 Local number length = 7 Public received number length = 3 Thus the first four digits are deleted by the system.
ONN blocking state	Suppression bit, Service code	Set the Outgoing Name and Number (ONN) Blocking. When you activate ONN, a user can press [*] [8] [1] [9] to block the outgoing name and number on a per call basis. The system flags the call to the Central Office (CO) so that the name and number is not sent to the person you call.

Table 18 Loop settings (Continued)

Attribute	Value	Description
Sampling (S loop only)	Adaptive, Fixed	Select a sampling rate for the S-loop. Fixed: two or more S-interface devices use the loop, and the length of the loop is less than 200 m (650 ft.). Adaptive: two or more S-interface devices use the loop, and the length of the loop is greater than 200 m (650 ft.).
		Note: If one S-interface device is using the loop, the length of the loop can be a maximum of 1000 m (3230 ft). The Sampling rate must be set to Adaptive.

SPIDs (NI only)

For ISDN BRI service, your service provider supplies service profile identifiers (SPIDs) and Network DNs. You need to assign a SPID to a loop before you can assign DNs to that loop.

Note: NI stands for National ISDN Protocol, which is used for profiles outside of North America. This protocol is not used with the ETSI protocol.

To assign an SPID to a BRI loop:

1. Choose **Services**, **Telephony Services**, **Loops.**
2. Click the key beside the loop number (for example, Loop 201) where you want to assign DNs.
3. Click the **SPIDs** heading.
4. Click the **Add** button.

   The SPID dialog box appears.
5. Type in the SPID number.
6. Click **Save**.

   SPID 1 appears as a sub-heading.

Assigning the Number of B channels

Each loop has two B channels. You can assign a different SPID to each channel, or you can assign the same SPID to both channels. SPIDs are supplied by your service provider when you are assigned the ISDN lines.

To assign the number of B channels to a SPID:

1. From the **SPIDs** heading, click the **SPID #** you want to configure for this Loop.
2. Select **1** or **2** in the **Number of B-channels** box.

Assigning DNs

To assign Network DNs to the BRI loop:

1. From the **SPID #** heading, click the **Network DNs** heading.
2. Click the **Add** button above the navigation tree.
3. Type the DN number in the **DN** box.
4. Click the **Save** button. **DN 01** appears as a sub-heading.
5. Repeat for all the DNs you want to associate with the loop.

Assigning Call type for a Network DN

Configure the call type for the Network DN, **Voice**, **Data** or **Both**:

1. From the **Network DNs** heading, click the **DN ##** that you assigned.

   The **Loop# /SPID# /DN #** window appears.
2. In the Call type field, select **Voice**, **Data** or **Both**.

Loop Matrix

To help you with your loop planning, transfer the following information to a spreadsheet and fill out the values for each BRI loop.

Table 19 Loop attributes

Protocol	
Overlap receiving	
Local number length	
ONN blocking state	
Sampling (S loop only)	
Note: The loop type dictates which fields appear.	

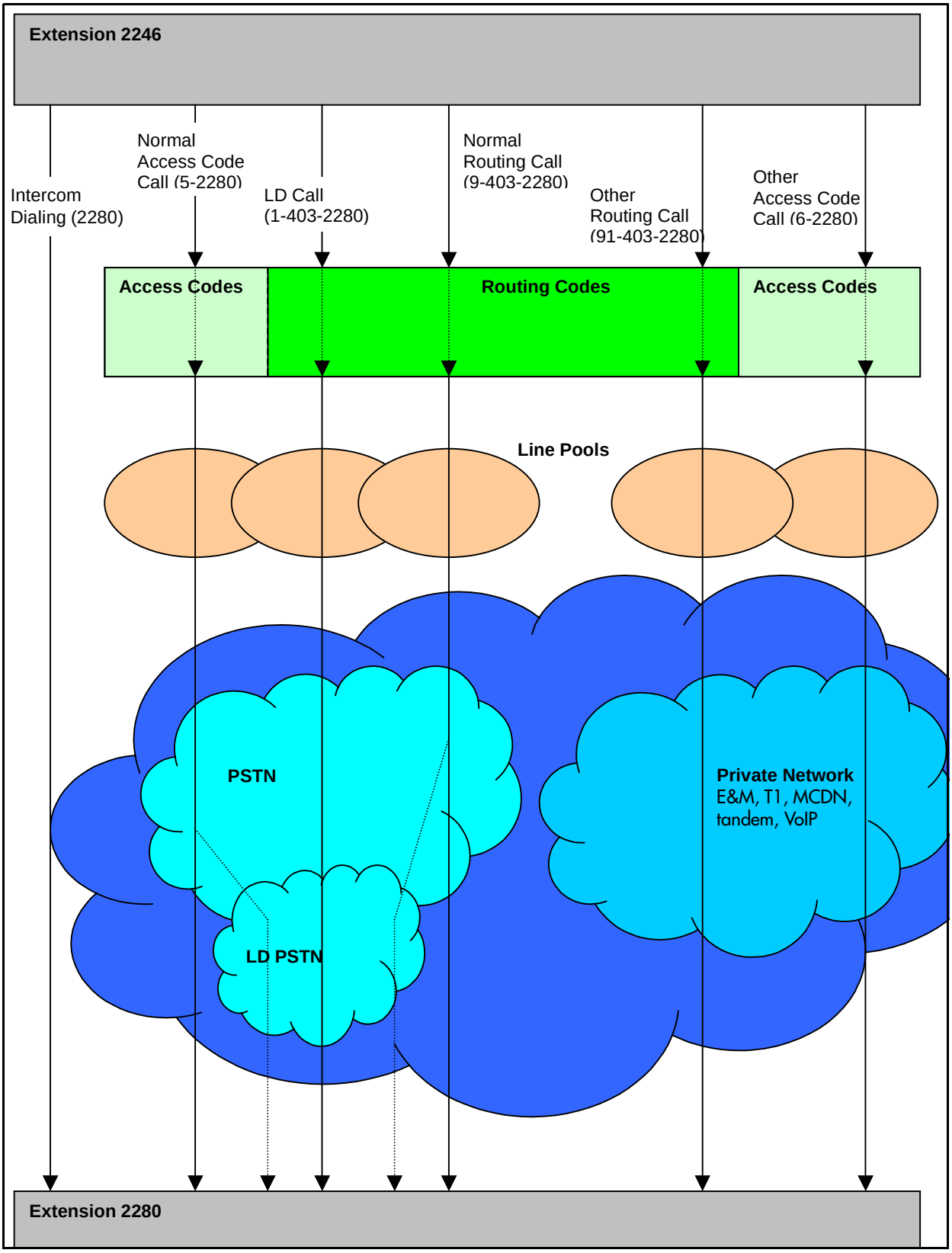
Determining Line Access

The next two sections, “Configuring Access Codes” on page 111 and “Configuring Call Routing” on page 117 describe what you do with the lines and loops you set up in the previous sections.

By using access codes or call routing, which uses destination codes, you can determine where lines go and how users access the lines. When you create a route, you can also specific restrictions that apply to how or when the line will be used.

Figure 16 on page 110 provides an overview of how access codes and routing is used within the system to direct calls from a telephone in one system to a telephone in another system.

Figure 16 Describing line management



Configuring Access Codes

The system uses Access codes to direct calls to the correct lines and destinations. If the codes conflict, some of the features on the system do not work.

Task:

Set up access codes for any or all of the following:

- park prefix
- external code
- direct dial digit
- auto DN
- DISA DN
- private access code

The table of default settings shown in Table 20 can help you plan your access codes so there are no conflicts.

Table 20 Default codes table

Digit	Use	Heading
0	direct dial digit	Access codes
1	park prefix	Access codes
2	first digit of B1 DNs	Set through Quick Start Wizard
9	line pool A access code (Takes precedence over the External line access code if there is a conflict.)	Access codes
— —	external line access code	Access codes
— —	destination code	Call Routing

Programming Access Codes

Your system requirements will determine which access codes you need to set up.

Follow these steps to set up access codes:

1 Choose **Services**, **Telephony Services**, **General Settings**

2 **Click on Access codes**.

The Access codes window appears.

3 Use Table 21 to determine which values to set for access codes for your system.

Note: Read the Tips boxes for each variable marked with an asterisk (*) before you choose a value to ensure the value does not conflict with related variables.

Table 21 Access codes values

Attribute	Values	Description
* Park prefix	None <one-digit number>	The Park prefix is the first digit of the call park retrieval code that you enter to retrieve a parked call. If the Park prefix is set to None, calls cannot be parked. Refer to "Tips About Access Codes" on page 112 before choosing a number.
* External code	None <one-digit number>	The External code setting allows you to assign the external line access code for T7100 telephones and ATA 2s to access external lines. Refer to "Tips About Access Codes" on page 112 before choosing a number.
* Direct dial digit	None <one-digit number>	The Direct dial digit setting allows you to specify a single system-wide digit to call a direct dial telephone. Refer to "Tips About Access Codes" on page 112 before choosing a number.
* Auto DN	<DN digits to be received from the auto-answer trunk>	Calls answered without DISA require no password to access Business Communications Manager. The Class of Service (COS) that applies to the call depends on the COS for the trunk.
* DISA DN	<DISA DN digits to be received from the auto-answer trunk>	For calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (COS) that applies to the call is determined by this COS password. After a remote user accesses Business Communications Manager, they can change the existing COS using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access and separate COS passwords with different dialing out privileges for individuals.
Private access code	<two-digit access code>	The Private access code is the first digit the user dials to access private facilities. It provides access to tandem and toll bypass functionality. For example, a PSTN user in Toronto could call a PSTN user in Ottawa and have the call routed over the private network connection from the Toronto office to the Ottawa office and then out to the PSTN from the Ottawa office. This bypasses any long distance toll charges. To add this functionality, the destination code has to include the private access number.

Tips About Access Codes

Here are some helpful pointers to assist you in planning the access codes for your system.

- The **Park prefix** cannot be the same as:
  - direct dial digit
  - external line access code
  - first digit of a DN
  - first digit of a line pool access code
  - first digit of a destination code

Other programmable settings may affect what numbers appear in the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may already be assigned elsewhere by default or by programming changes.To avoid a conflict, refer to the table of default settings in the description of External code.

If the DN length changes, and the changed DNs conflict with the Park prefix, the setting changes to None.

- The **external line access code** cannot conflict with:
  - Park prefix,
  - direct dial digit
  - first digit of a line pool access code
  - first digit of a DN
  - first digit of a destination code

  If the DN length is changed, and the changed DNs conflict with the external line access code, the setting changes to None.
- Another **direct dial** telephone, an extra dial telephone, can be assigned for each schedule in Services programming.

  The Direct dial digit cannot be the same as the:
  - first digit of a DN
  - first digit of a line pool access code
  - first digit of a destination code
  - external line access code
  - Call park prefix

  If the DN length is changed, and the changed DNs conflict with the Direct dial digit, the setting changes to None.
- The length of the **Auto DN** is the same as the Received Number Length specified in **General Settings**. The Auto DN is cleared if the Received Number Length is changed.

  The Auto DN cannot be the same as a:
  - line pool access code
  - destination code
- The length of the **DISA DN** is the same as the Received number length specified in **General Settings**. The DISA DN is cleared if the Received number length is changed.

  The DISA DN cannot be the same as a:
  - line pool access code
  - destination code

Line Pool Access Codes

Line pool access codes allow you to assign an access code for each of the 15 line pools (A to O). These codes specify the line pool for making an outgoing external call.

Follow these steps to set line pool access codes:

1. Choose **Services**, **Telephony Services**, **General Settings**, **Access codes**.
2. Click the key beside **Line pool codes**.

   Pool A-Pool O appears on the navigation tree.
3. Click the Pool you want to program.

   The Pool window appears.
4. Type the Access code.

   The default Access code is **9** for **Line Pool A**.

   There is no default Access code for Line Pools B to O.

You cannot assign PRI line pools with a line pool access code. You must define PRI line pools under routing, and create destination codes for the routes..

Tips: The code can be one to four digits.

A line pool access code can be the same as an external line access code. In this case, the line pool access code takes priority over the external line access code, and a line from the line pool is selected.

A line pool access code cannot conflict with:

- park prefix
- direct dial digit
- first digit of any received number
- first digit of any DN (including the Auto DN or the DISA DN)

To avoid a conflict, refer to the table of default settings in the description of External code.

Note: VoIP lines

Although VoIP lines are not physical lines, you can create a line pool and line pool access codes to access this service.

The VoIP keycode must be enabled before you can access any VoIP lines.
The VoIP keycode on a remote target Business Communications Manager must also be enabled for that system to receive VoIP-based calls from your system.

For detailed information about VoIP lines, refer to the *IP Telephony Configuration Guide.*

Using Carrier Codes

A multi-digit Carrier access code contains an Equal Access Identifier Code (CAC) followed by a Carrier Identification Code (CIC). The CIC identifies the carrier that handles the call. The Carrier Access Code table stores the CAC digit pattern that you define for your region.

In most cases it is not necessary to change the default values.

About Carrier Access Codes

Here are some general points about carrier access codes:

- You can define up to five carrier codes.
- Two entries will be pre-defined in North America, but you can remove these defaults.
- Each entry consists of an equal access identifier code prefix (one to six digits) and a carrier identification code length (one digit, 1 to 9).
- Each entry is identified by the prefix digits themselves.

Identifying Carrier Access Codes

1. Select **General settings/Access codes/Carrier codes**.
2. Click a Prefix number, or choose **Add** from the buttons above the navigation tree to add a new Prefix.
3. Use Table 22 to determine which values to set so callers can access a private network.

Table 22 Carrier access code values

Attribute	Values	Description
Code prefix	<one to six digits>	This value defines the prefix that will be used to access the carrier code.
ID length	1, 2, 3, 4, 5, 6, 7, 8, or 9	This value defines the carrier ID length.

Access Code Matrix

To help you with your Access code planning, transfer the following information to a spread sheet and fill out the access codes you want to use.

Table 23 Access code values

Line pool codes	A: **9** B: _____ C:_____ D:_____ E:_____ F:_____ G:_____ H:_____ I: _____ J: _____ K:_____ L:_____ M:_____ N:_____ O:_____
Park prefix	0 **1** 2 3 4 5 6 7 8 9 None
Extrnl code	0 1 2 3 4 5 6 7 8 9 **None**
Direct-dial digit	**0** 1 2 3 4 5 6 7 8 9 None
Auto DN	**None** Received #_____
DISA DN	**None** Received #_____
Private Access Code	0 **1** 2 3 4 5 6 7 8 9 None

Carrier Codes	
Code prefix	ID length: 0 **1** 2 3 4 5 6 7 8 9 None

Configuring Call Routing

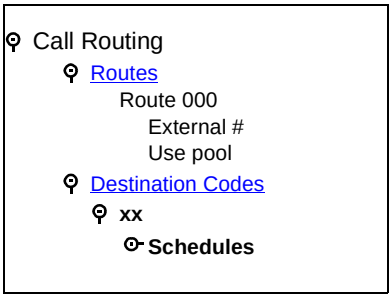
Call Routing allows you to define how calls are routed by your Business Communications Manager system.

Task:

- Set up routes to external numbers using a specific line pool
- Enter destination codes to key access to a route
- Assign schedules for each route

Figure 17 shows a detailed view of the Call Routing programming map.

Figure 17 Call Routing headings



About Call Routing

Call routing decides what path an outgoing call takes using the digits that are dialed. It is sometimes called Automatic Route Selection (ARS).

When you select an internal line and dial, the system checks the numbers you enter against the routing tables. If the number you dial starts with a destination code, the system uses the line pool and dials out digits specified by the route assigned to that destination code, and then dials the rest of the number that you dialed.

Routing service replaces a number of manual tasks, including:

- entering a line pool code
- dialing an access code for a long distance carrier
- deciding which line pool to use according to the time and day

You can set up routing to take advantage of any leased or discounted routes using information supplied by the customer. The system cannot tell what lines are cheaper to use.

For Call by Call service selection (PRI only), the installer defines destination codes for various call types over PRI lines (for example, Foreign Exchange, Tie Trunk, or OUTWATS). The user dials a number using the intercom button without entering any special information. For more information see, “Provisioning for Call by Call Limits with PRI” on page 188.

Using routing to create a coordinated dialing plan is explained in “Using a Dialing Plan to Route Outgoing PRI Calls” on page 128.

Warning: Plan your routing service before you do any programming. Routing affects every call placed in the system and must be carefully planned to avoid conflicts and gaps in the programming. Use tables to design routes and destination codes, then check for potential problems before you start programming. It also saves you time when all the settings are written out in front of you.

Routes and Destination Codes

The settings for a call route include:

- a three-digit route number (000-999)
- external # digits (up to 24)
- a line pool
- destination codes (max. of 500 available, up to 7 digits)
- DN type
- public DN lengths
- a schedule (programmed in Services)

Tips
To dial a telephone number that does not match a programmed destination codes, you must choose a line and dial the number. For long distance dialing, you can program the area codes in the North American numbering plan as destination codes.

Avoiding Routing Conflicts

The codes you choose for the following must be unique. Use Table 24 to plan your access codes.

Table 24 Avoiding code conflicts

Access codes	Values or range
Destination codes	
Call Park Prefix	
External Access Code	
Direct Dial Numbers	
Line Pool Codes	
Internal set DNs	
DISA DNs	
Auto DNs	

Defining Routes

Use the Routes command to configure route records that are assigned to telephones.

1. Choose **Services/Telephony Services**.
2. Click the key beside **Call Routing**.
3. Click **Routes**.
4. Click the **Add** button.

   The Add Routes dialog box appears.
5. Enter a three-digit route number (001-999).

Note: Route 000 is a default route and cannot be changed or deleted.

6. Click **Save**.
7. Click the **Route** number in the navigation tree.
   The Route window appears.
8. Use the information in Table 25 to configure the route settings.

Table 25 Route settings

Attribute	Value	Description
External #	a maximum of 24 digits	Enter the external or dial-out number for the route you want the assigned telephone to use. Optional entries: F78: 1.5 second pause (counts as one digit in the dialing string) F804: wait for dial tone (counts as two digits in the dialing string) F71: Link F808: Long tones F*89: Programmed release F*9: Run/Stop Leave this entry blank if the route is directed to a VoIP line pool.
Use pool	Pool A to Pool O or PRI-A to PRI-F	Select a line pool for the route. The PRI pools only display if you configure an DTM for PRI.
DN type (only for Tie lines)	Public Private	This determines whether the call will use the public DN length to route a call through the public network, or the Private DN length to route the call through the private network.

Call by Call Service Routing

Table 26 provides an example of a Routing Table containing Call by Call programming (available in the North America market profile).

Table 26 Call by Call routing table example

Route # (000-999)	Dial Out (24 digits)	Use Pool	Service Type	Service Identifier
003		PRI-A	Public	
004		PRI-A	FX	xxxxx
005		PRI-A	Tie	xxxxx
006		PRI-B	OUTWATS	xxx
007		PRI-B	Private	
008		PRI-B	Switched Digital	

Note: The public DN lengths are used for all PRI calls except those whose routes use service type Private or service type Tie with DN Type specified as Private.

The service identifier (SID) depends on the selected service type (for example, with NI-2 protocol).

Service Type	Service Identifier description
Public	None
FX	Facility Number 1-5 digits
Tie	Facility Number 1-5 digits
OUTWATS[a]	Optional Band Number 1-3 digits
Private	None
Switched Digital	None

a. For NI-2, do not program the Carrier Access Code for banded OUTWAT calls. This call may be rejected.

When you select or change a PRI protocol, the Service Type and Service ID fields automatically clear for each entry in the routing table for that PRI.

Programming the PRI Routing Table

The dialing plan must be thoroughly planned out in advance before programming the information into the Business Communications Manager system.

To program the routing table:

1. Choose **Services**, **Telephony Services**, **Call Routing**, **Routes**.
2. Click on the route number record you want to use.
3. Beside **External #:**, type a number (up to 24 digits).
4. Under **Use pool,** select a line pool.

   The PRI pool(s) displayed depend on how you allocate PRI lines into pools in the **Trunk/Line Data** section of line programming. It is possible to have only pool PRI-A, or only pool PRI-B, or only pool PRI-C, etc., even if there are three DTMs configured as PRI in the system.
5. Under **ServiceType:Public**, select a different Service Type if required.
6. Under **Service ID:None**, type the Service ID number.
   This field appears only if the service requires an ID.
7. Under **DN type: Public** or **Private**. This box appears only for the Tie service type.

Programming Destination Codes

The numbers used for destination codes must not conflict with the following:

- call park prefix
- external access code
- direct dial numbers
- line pool codes
- internal telephone DN (intercom)
- DISA DN
- auto DN

For example, the system will confuse an internal number of 221 and a destination code of 22, because the system routes the call based on the first digits dialed. When the caller dials 221 to reach an internal telephone, the system sees the first two digits (22) and routes the call using destination code 22. An internal number of 221 and a destination code of 23 would work.

To make digits available for use with destination codes, you can change the DN length of B1 and B2 DNs depending on your system size. You can change the DN length either at system startup or in **General settings**.

Wild Card Character

When programming destination codes, you can use wild cards in the destination code string. Wild card characters reduce the number of destination codes programmed in the system.

The wild card character can only be used to group destination codes that use the same Route and Digit Absorbed Length.

1 Choose **Services**, **Telephony Services**, **Call Routing**.

2 Click on **Destination codes**.

3 Click on the destination code you want to modify, or click on the **Add** button**.**

The Destination code dialog box appears.

4 When you enter a destination code, type the letter A as a wild card character for the last digit of the destination code.

Note: The wild card character can be used only for the last digit of a destination code and represents any digit from 0 to 9 except for digits already programmed or used by other numbering plans. If there is a conflict with other digits already programmed or used by other destination codes, an error message appears.

5 Click on the key beside **Schedules**.

6 Click on the schedule name you want to program. For example: Normal.

7 Choose the **Use route** you want the destination code to refer to during operation of the schedule.

8 In **Absorb Length**, choose a number to define which part of the destination code will be ignored by the system when it dials out. Table 27 demonstrations this process.

Table 27 Destination codes without wild cards

Destination codes	Digit Absorb	Route	Route external #	Number Dialed Out
9201[1]	3	555	763-4018	763-4018 *-1*
9202	3	565	763-3492	763-3492 *-2*
9203	3	555	763-4018	763-4018 *-3*
9204	All	555	763-4018	763-4018
9205	2	565		763-3492 *-05*
9206	3	555	763-4018	763-4018 *-6*
920A	3	555	763-4018	763-4018 - A

1 In this example, the default Line Pool A access code 9 is deleted to make it available for use as a Destination code.

Note: The numbers in italics in the Dial Out sequence are not visible to the user.

Tips

The digit absorption setting (absorbed length) applies to a maximum of two schedules. To minimize the effort involved in preparing destination codes, set the digit absorption to 0 . With a 0 setting, the actual digits dialed by a caller are preserved in the dial out sequence. The need to program a dial out sequence as part of the route depends on the required dialout.

Setting Up a Route for Local Calling

An office can have different suppliers for local and long distance telephone service. By programming a destination code, any call that begins with 9, which is the most common dial out digit, automatically uses lines dedicated to local service.

Note: 9 is the default setting for the line pool code for Pool A. If you want to use 9 as a destination code, you must change the Pool A code. Refer to "Assigning Line Pool Access" on page 155.

Follow these steps to build a route to allow local calls.

1 The first step is to build a route (under **Call Routing in Telephony Services**).

   a Type in a route number.

   b Choose the line pool that was defined for the lines for local calling.

   c Type the dial out digits, if any, required to direct the call once it is connected to an external line.

2 The second step of programming is setting up how the route will work with a destination code. Because users will dial 9 to make an external call, 9 should be the destination code.

   For local calls only, there are no dial out numbers (compare with "Setting Up a Route for Long Distance Calling" on page 125).

   a Beside **Destination Code**, type 9.

   If you enter a code other than 9, you must use a valid destination code. See "Programming Destination Codes" on page 122. View existing destination codes before entering a new code.

   The destination code can use a different route depending on what schedule is assigned. In the current example, the route you defined is used when someone dials 9 during Normal mode, when the other Schedules are turned off.

   b The route for the first schedule appears after **Normal:**. Type the defined route number.

   Figure 18 shows an example of a Routing service programming record.

   Figure 19 shows an example of a Destination codes programming record filled out for the two routes created in Figure 18.

Figure 18 Routing Service programming example

Routing Service (Services: Routing Service)		
Route # (000-999)	**Dial out** (if required) (max. 24 digits or characters)	Use Pool
001	none	(A) B C D E F G H I J K L M N O
002	none	A (B) C D E F G H I J K L M N O

Figure 19 Destination codes for call routing

Destination codes (Services; Routing service; Destination codes)								
Service Schedule name (max. 7 char)	Normal Rte		**Night Rte**		**Evening Rte**		**Lunch Rte**	
DestCode (max. 7 digits)	Use route (000-999	Absorb Length	Use route (000-999	Absorb Length	Use route (000-999	Absorb Length	Use route (000-999	Absorb Length
9	003	All						
1	002	0						

Setting Up a Route for Long Distance Calling

An office can have leased lines or private network trunks that provide cheaper to long distance calls by routing through the dedicated lines to remote systems, then using the local PSTN from that system to make the call. The routing should take place automatically when the number of the outgoing call begins with 1.

Follow these steps to set up a route through a dedicated trunk:

1. Beside **Route:** enter a valid route number.
2. Choose the line pool that contains the discounted lines for calling long distance.
3. Beside **Destination Code:** enter a unique code number.

   You must use a valid destination code. See "Programming Destination Codes" on page 122. View existing destination codes before entering a new code.

   The destination code can use a different route depending on the Schedule.
4. Under the **Normal** schedule for the destination code, type the route you specified in steps 1 and 2.

Tips

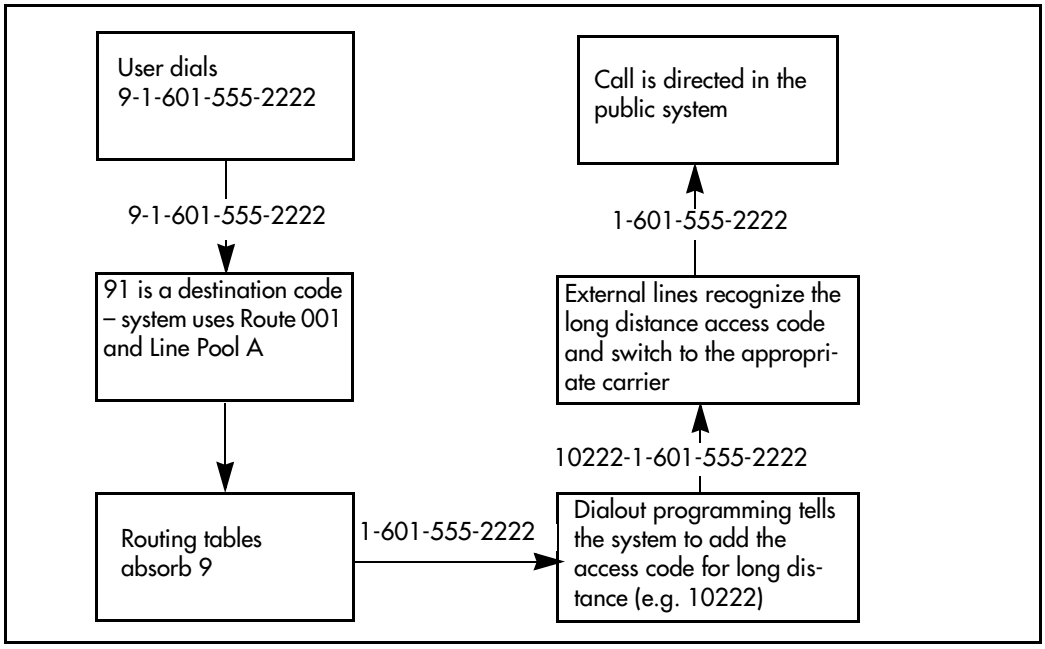
The digit absorption setting (**Absorbed Length**) applies to a maximum of two schedules.

Setting **Absorbed Length** to 0 minimizes the effort involved in preparing destination codes. When the Absorbed Length is at 0, the actual digits dialed by a caller are preserved in the dialout sequence. It is not necessary to program a dial out sequence as part of the route.
If rates change depending on the time of the day or week, a different route can be used for the same destination code when a particular schedule is in use. See "Programming for Least Cost Routing" on page 127.

Adding a Long Distance Carrier Access Code

In many cases, long distance service uses the same lines as local service but is switched to a specific carrier using an access number, which is sometimes referred to as an equal access code. Route programming can include the access number so the users do not have to dial it every time they make a long distance call. Refer to Figure 20.

Figure 20 Carrier code call numbering sequence


User dials
9-1-601-555-2222
9-1-601-555-2222
91 is a destination code – system uses Route 001 and Line Pool A
Routing tables absorb 9
1-601-555-2222
Dialout programming tells the system to add the access code for long distance (e.g. 10222)
10222-1-601-555-2222
External lines recognize the long distance access code and switch to the appropriate carrier
1-601-555-2222
Call is directed in the public system

Follow these steps to program a long distance carrier access code into a destination code.

1. Create a route that uses a line pool containing local lines only.
2. Program the route to use a line pool containing the lines used to access the long distance carriers.
3. Type the dial-out digits, which are the same as the access digits. For example, if the access code is 10222, the dial-out digits are 10222.
4. Create a destination code 91: 9 (for outside access) and 1 (for long distance).You must use a valid destination code. Refer to “Programming Destination Codes” on page 122.
5. Set **Absorbed Length** to 1.

   The digit 9 is only used internally and should be dropped. The 1 is needed to direct the call to the public carrier network.

Tips
The destination codes 9 and 91 used in the examples cannot be used together. If you need the destination code 91 to direct long distance calls, you must create a separate set of codes that use local calling routes. These codes would be, for example, 90, 92, 93, 94, 95, 96, 97, 98 and 99. Refer to “Wild Card Character” on page 122 for information on programming destination codes.

Programming for Least Cost Routing

It can be less expensive to use another long distance carrier at a different time of day. Continuing with the example used in the previous flowchart, the lines that supply local service in normal mode are also used for long distance service after 6 p.m. because that is when rates become competitive. For the system to do this automatically, you must build another route.

Follow these steps to build a route for a secondary carrier:

1. Beside **Route:** enter an available route number.
2. Choose **No number** for the dial out.
3. Choose the line pool that contains the local service carrier lines.
4. Now you need to create a destination code and assign the route to the Night schedule.

   In this case, the change in route uses the start and stop times for Night Schedule.
5. Add 91 as a **Destination code.**
6. Make sure **Absorbed length** is set at 1.
7. Under **Night schedule:** enter the route you defined in step 1.

Calls that begin with the digits 91 travel out without using the access code when the Night schedule becomes active or when you turn it on at a control telephone.

Overflow Routing

If all the lines used by a route are busy when a call is made, you can create a route that automatically picks up the call. However, this only takes effect if an active schedule is applied to the line. Overflow routing is not available in Normal mode.

You must create a separate overflow route for each destination code for which you want to allow overflow routing.

To set up the overflow feature:

1. You assign the preferred route in a Destination code schedule (Services/Telephony Services/ Call Routing/Destination code). In this preferred route schedule, you define the start/stop time as 0100. In this case, that means the schedule is active 24 hours a day. Pick a schedule that you do not use for any other purpose, such as Sched 4.
2. You assign the overflow route to the same Destination Code, but for the Normal schedule.
3. Under **Scheduled Services/Routing Service/<preferred route schedule>**, choose **auto** for **Service Setting,** and **Y** for **Overflow**.
4. Use a control telephone to activate the feature on the telephones on which you want preferred routing to be active. The telephones must be assigned both the preferred line pool, and the overflow line pool.

5 You must also ensure that the route correctly aborbs or passes dialed digits so that the number dialed for each line is the same from the user perspective.

When a user dials, and the telephone cannot capture the preferred line, the telephone reverts to the Normal mode, which uses the fallback route to make the call.

Note: Overflow routing directs calls using alternate line pools. A call can be affected by different line filters when it is handled by overflow routing.

VoIP trunking uses a similar process for setting up fallback from the VoIP trunk to a PSTN line. Refer to the *IP Telephony Configuration Guide* for details.

Using Dialing Restrictions with Routing

You can further customize routing service by adding dialing filters to lines in line pools. Filters restrict the use of the line to specific area codes.

Tips: Host system signaling codes can be part of the dial out.
You can also use routing as an alternate method for a direct-dial number. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Set the digit absorption to 1.

Using a Dialing Plan to Route Outgoing PRI Calls

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing outgoing calls. All PRI calls must go through a dialing plan.

The Dialing Plan:

- Allows Enbloc dialing by buffering user-dialed digits until a complete DN has been dialed. Enbloc dialing is a requirement for PRI.
- Provides the ability to map user-dialed digits to a service type on a call-by-call basis.
- Allows long distance carrier selection via user-dialed Carrier Access Codes.
- Allows incoming calls to be routed according to the service type and the digits received.

Enbloc Dialing

Enbloc dialing allows the system to determine where a call should be routed on a PRI line. By not dialing out until all digits are entered, the system looks at the entire code and can tell whether the call should be routed through public lines, to another system on a network through private lines, or to the local system.

Public and Private DN lengths and destination codes are used by the system to determine routing. Any prefixes that need to be added on the dialed number, can be included in these settings.

Routing Matrix

To help you with your route planning, transfer the following information to a spreadsheet and fill out the values for each route you create.

Table 28 Routing

Call Routing: Routes			
Route #	External #	Use Pool	DN type Public Private
Destination code:	Normal Night Evening Lunch Sched 4 Sched 5 Sched 6	Use route None Route: Route 001	Absorb length All 1 2 3 4 etc. _____

System Line Settings

A number of line settings affect the entire system and must be coordinated with other settings.

Network Name Display

Business Communications Manager displays the name of the calling party, when available, on both Private or Public ISDN PRI interfaces. The displayed name can include the Receiving Calling Name, Receiving Redirected Name, and/or Receiving Connected Name. The outgoing name is the Business name and the telephone name. The outgoing name is not supported on BRI (North America). Table 29 provides a list of the name/number display features and the list of ISDN interfaces that support each feature.

Table 29 Call features/interface list

	Interface			
Feature	**NI PRI**	**DMS Custom PRI**	**SL-1 (MCDN)**	**NI-BRI**
Receiving Calling Name	Supported	Supported	Supported	Supported
Receiving Redirected Name	Supported		Supported	Supported
Receiving Connected Name		Supported	Supported	
Sending Calling Party Name	Supported	Supported	Supported	
Sending Connected Name		Supported	Supported	

Note: Network Name Display is an optional feature that is available based on the interface you subscribe to.

MCDN note: MCDN networks fully support name display features.

Receiving and Sending Calling Party Name

Network Name Display allows the name of an incoming PRI/BRI call to appear on the Business Communications Manager telephone receiving the call.

Calling Party Name with status of PRIVATE can appear on the Called Party telephone as **Private name**. If the incoming Calling Name is defined by the CO as a private name, then **Private name** appears on the answering telephone. If the Calling Party Name is unavailable it can appear on the Called Party telephone as **Unknown name**.

If the call is answered by a hunt group, the hunt group name appears instead of the telephone name in forming the connected name.

The Connected Name is a transient display that appears for approximately three seconds.

Note: The Connected Name is sent only if the OLI is programmed.

Network Name Display interactions

Calling and Connected Name information (if available) passes between trunks with Selective Line Redirection (SLR). Only Calling Name information passes between trunks in cases where Direct System Inward Access (DISA) results in tandeming of trunks.

Programming Network Name Display

Nortel Networks recommends that you use a blank space for the last character of the Business name to act as a separator between the Business name and telephone name.

Note, that if you leave this field blank, no name appears.

To program the Business Name:

1. Under **Services/Telephony Services,** click on **General Settings.**
2. In the **Business name** box, type the Business name you want to appear on receiving telephones (a maximum of seven characters).
3. Other areas that you must programmed include:
   - The **OLI number**. Refer to “Assigning Line Access” on page 150.
   - Under **Telco Features**, the **Call ID** must be set to **Yes**. Refer to “Configuring Telco Features” on page 169
   - Under **Lines**, type the telephone number where you want the **CLID** to appear. Refer to “Assigning Trunk/line Data” on page 97.

Remote Access Line Settings

The remote access feature allows callers elsewhere on the private or the public network to access Business Communications Manager by dialing directly and not going through the attendant. After the remote user is in the system, they can use some of the system resources. You must enable remote access in programming before callers can use it.

Business Communications Manager supports remote system access on a number of trunk types which may require the remote caller to enter a password for direct inward system access (DISA).

The system resources, such as dialing capabilities, line pool access and feature access, that a remote user may access depends on the Class of Service (COS) assigned to them. See "COS Passwords" on page 184 and the *Business Communications Manager Feature Programming Telephone Guide* for more details.

Note: To use features on Business Communications Manager remotely, press * followed by the Feature code. Even if you are calling from another Business Communications Manager system, press * instead of .

Remote Access on Loop Start Trunks

Loop start trunks provide remote access to Business Communications Manager from the public network. They must be configured to be auto-answer to provide remote system access.

A loop start trunk **must** have disconnect supervision if it is to operate in the auto-answer mode. T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer, the system answers with system dial tone and no (COS) password is required. In this case, the restriction filters assigned to the line control system capabilities available to the caller.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a COS password that determines which system capabilities are available to the caller.

Remote Access on a Private Network

Systems connected to the private network deliver the last dialed digits to the destination Business Communications Manager system for interpretation. The destination Business Communications Manager system matches the digits to a target line or interprets the digits as a remote feature request. Business Communications Manager then routes the call to the specified target line or activates the remote feature.

By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are **not** answered with DISA.

If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a COS password.

The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA. These DNs are described in "Programming Access Codes" on page 111.

Remote Access on T1 DID Trunks

Remote system access on T1 Direct Inward Dial (DID) trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- A remote caller is on the public network dialing standard local or long distance telephone numbers.
- The digits received are delivered by the central office.
- DISA cannot be administered to a T1 DID trunk.

You can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN.

Remote Access on PRI Trunks

Remote system access on PRI trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- A remote caller is on the public network dialing standard local or long-distance telephone numbers.
- The digits received are delivered by the central office.
- Answer with DISA cannot be administered to a PRI trunk.

You can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN.

Remote Access on DPNSS Lines

A remote caller can access a Business Communications Manager system dial tone, select a line pool that contains exchange lines or DPNSS lines, then dial a number. The procedure is identical to dialing an outside number from an extension in the local system. The main features are:

- Calls coming from another switch to the Business Communications Manager system are routed in two ways, depending on the Answer mode that you program. If the Answer mode is set to Manual and the line is assigned to ring at an extension, the incoming call automatically rings at the assigned extension. If Answer mode is set to Auto, Business Communications Manager automatically answers the incoming call. Because most other DPNSS features are extension specific, Nortel Networks recommendeds that all DPNSS lines are configured as Auto-answer lines.

- The Page feature is available to both remote callers and callers within the system. A remote caller must have DTMF capability to access the Page feature.
- The Line Redirection feature allows the originating party to redirect a call that is waiting a connection or re-connection to an alternate destination after a time-out period. Failed calls can be redirected. Priority calls cannot be redirected.

Chapter 7
Configuring System DNs

This chapter describes the programming for the sets attached to the station modules on the Business Communications Manager.

Task:

Set up each telephone line.

- Determine which DNs will be assigned to telephones.
- Assign lines or line pools to each telephone
- Determine the Capabilities and User Preferences
- Determine the restrictions for each telephone.
- Determine the schedule for each telephone.

Note: References in this document to *Terminal*, *set*, and *telephone* all refer to telephones that are compatible with the Business Communications Manager system.

About System DNs

There are two sides to DNs that affect system telephones and equipment.

- On the system side, each telephone on the network is assigned a DN number, which identifies it to the system. DNs for digital telephones map to each wire pair on a station media bay module. IP telephones can be assigned a DN from the range of DNs designated for digital telephones. ISDN and DECT terminal DNs map to defaults determined by ISDN programming. Similarly, the Companion programming determines the range of DNs available to the Companion sets (NA portable).

  When you initialize your system, you will be asked to specify a DN length and a Start DN.

  This chapter discusses set DNs in terms of a default Start DN of 221, and a DN length equal to 3. You can specify different lengths of DN or an entirely different Start DN, depending on your system requirements.

  You can renumber a group of DNs after you initialize your system. For example, if your service provider has given you a specific list of DID numbers, you might choose to ensure the DNs mirror those numbers, to make it easier to administer the telephones. The DN Renumber Wizard allows you to accomplish this quickly. Refer to "Using a Wizard to Renumber Telephone DNs" on page 139. If you do this after you have programmed telephones to the DNs, the programming attached to the original DN is transferred to the new DN.

  To view your system settings: Click on **Diagnostics/MSC**, then select **Configuration** and click on **System Startup**. This screen displays the telephony template that is active for your system and the start DN that is assigned to the system.

Warning: Changing the DN length after system startup:

Changes to set DN length can affect other applications. Make changes to the Start DN or the system DN length at system installation, before you do any other programming.

- The second part of a DN, is the content of the DN record. Each DN heading provides a number of parameters that get assigned to the telephone that accesses that DN. Some of these parameters can be copied to other telephones, while others, such as the name of the telephone, and button programming, is unique to each DN record or to each type of telephone.

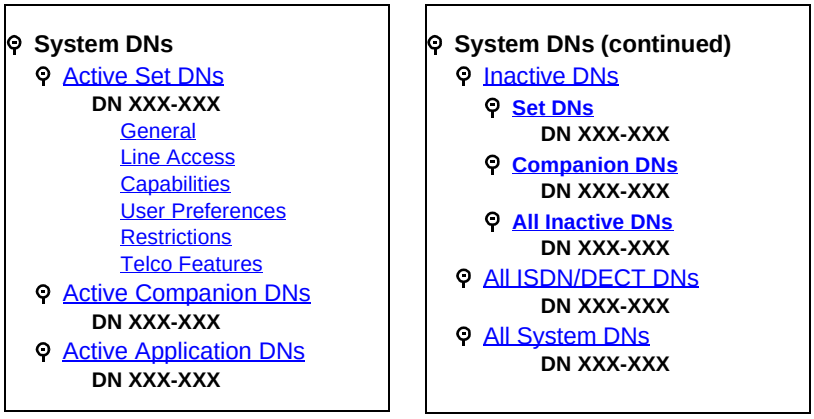
  DN content can be updated at any time, such as if you upgrade the model of telephone. For details about setting up or changing a DN record, refer to the sections in this chapter, starting with "Identifying the Telephone (General Heading)" on page 149.

Identifying System DNs

The System DN heading on the Unified Manager accesses four ways of viewing the system DNs. Refer to Figure 21.

This heading provides access to the DN records of telephones that are active on the system, records of all the DNs that are available, and a comprehensive list of all DN possibilities. Use the list that is most convenient for what you want to do.

Figure 21 System DNs main headings



Active Set DNs

This list displays only the DNs for digital, and IP telephones that are actually connected to the system and are activated. Use this list when you want to change a configuration, or remove a telephone.

Although IP telephone records are listed under this heading. Use this heading to access the IP telephone DN to create telephone capabilities, user preferences, and button programming. Refer to the *IP Telephone Configuration Guide* for details about IP telephone DN assignment.

Active Companion DNs

This list displays only the DNs for Companion sets that are registered on the system. Use this list when you want to change a configuration, or remove a telephone.

Note: This item only appears on the navigation tree for systems set to regions that support the Companion Wireless system. Refer to "Mobility Services by Region" on page 579.

Active Application DNs

This list segregates the list of DNs that are used for running applications, such as Voice Mail and Call Center. These DNs are assigned within the applications that they apply to. You do not need to do anything to any of these DNs, other than to note they are not available for application to your telephones.

Warning: Changing the settings on these DNs could cause malfunctions in the applications to which they apply.

Inactive DNs

The DNs listed in this section do not yet have telephones assigned to them.

Note: This list contains all possible DNs in the digital and Companion ranges. However, you can only assign a digital or Companion set to a DN that is connected to an installed station module. IP telephones can use any available DN in the digital range.

Set DNs

This list displays the digital telephone and IP telephone DNs that are not assigned or not active. Use this list to set up new telephones.

Companion DNs

This list displays the Companion DNs that do not have registered handsets. Use this list to define new handset records.

All Inactive DNs

This list displays all digital, IP, and Companion DNs that are not assigned or are not active.

Note: Companion DNs can also be used for DECT system that require more than the default number of ISDN and DECT DNs. In this case, when you define the Companion DN as ISDN and DECT, the record disappears off this list and appears on the All ISDN/ DECT DNs list.

All ISDN/DECT DNs

This list displays all the DNs that default to ISDN and DECT applications, plus any DNs from the Companion (NA Portable) range that have been changed to ISDN and DECT.

Note: ISDN and DECT DNs can also be used for Companion handsets that require more than the default number of Companion DNs. In this case, when you define the ISDN and DECT DN as NA Portable, the record disappears off this list and appears on the Active Companion DNs list.

All System DNs

This list displays all possible DNs, regardless of whether a station module is configured to activate them or not. This list begins with the Start DN.

Note: You can only assign a digital or Companion set to a DN that is connected to an installed station module. IP telephones can use any available DN in the digital range.

Table 30 provides a list of assigned DN numbers based on the default Start DN and the bus number (DS30 channel) the station module is set to. Use this list to indicate the DS30 channel and offset where you have station modules installed, and what DNs can be assigned.

If your system has a different Start DN or a different DN length, indicate your DN structure in the **DN assignment** column beside the bus # where you have assigned station modules.

Table 30 Default DNs, based on assigned bus number

Bus #	Type of module	Default DN numbers (based on default DN) Bus offset 0 1 2 3	DN assignment
		Default start DN: 221	New start DN:
02	Station module ASM DSM 4X16	 221-228 229-236 221-236 237-252 (Bus 03)	
03	Station module ASM DSM 4X16	 237-244 245-252 237-252 253-268 (Bus 04)	
04	Station module ASM DSM 4X16	 253-260 261-268 253-268 269-284 (Bus 05)	
05	Station module ASM DSM 4X16	 269-276 277-284 269-284 285-300 (Bus 06)	

Table 30 Default DNs, based on assigned bus number (Continued)

Bus #	Type of module	Default DN numbers (based on default DN) Bus offset 0 1 2 3	DN assignment
06	Station module ASM DSM 4X16 DECT	 285-292 293-300 285-300 (Companion system: 565-596) 301-316 (Bus 07) 501-624	
07	Station module ASM DSM 4X16 DECT	 301-308 309-316 301-316 (Companion system: 565-596) 221-236 (Bus 02) 501-624	

Feature DNs

The system also uses DNs to define remote access features and Hunt groups. These DNs do not show up on the System DNs list.

- System Access DNs: For remote access to direct-dial lines, the system requires that an Auto DN and a DISA DN. These two settings are found under the Access Codes heading. Refer to the remote access information in "Programming Access Codes" on page 111.
- Hunt Group DNs: Hunt Groups are identified by a unique DN for each defined Hunt Group. Refer to Chapter 13, "Configuring Hunt Groups," on page 285 for more information.

Using a Wizard to Renumber Telephone DNs

If you need to renumber any DNs, you can use the DN Renumber Wizard, which allows you to renumber a range of DNs.

Follow these steps to use the DN Renumber Wizard to renumber DNs on your system:

1. From the Programming Wizards page, enter the system user ID and password, then click the **DN Renumber** button.

   If you do not know how to access the Programming Wizards page, refer to "Accessing the Wizards" on page 60.

2. On the first screen, enter the range of DNs to change, and the DN with which to start re-numbering.
3. The **Summary** page displays the information you entered. Review and revise, if necessary.
4. Click the **Apply** button.

Warning: DECT DNs

Do not change DECT DNs after the DECT Configuration wizard has run. Doing so will make the DECT handsets inoperable until you reconfigure the DECT module and resubscribe the handsets.

Change Telephone DNs Using the Unified Manager

The General Settings heading also provides access to a screen where you can change the DN setting.

1. Click on the keys beside **Services**, **Telephony Services**.
2. Click on **General settings**.
3. On the top menu, click on **Configuration** and choose **Change DN**.

   The Change DN screen appears.
4. Click beside **Old DN** and enter the DN or group of DNs you want to change.
5. Click beside **New DN** and enter the DN or group of DNs you want to change to.
6. Click **OK** to start the change process.

Using Wizards to Control DN Records

There are two Wizards that allow you to set up basic telephone configurations and easily apply them to new telephones as they are added to your system.

Creating User Templates with the Edit Template Wizard

The Edit Template Wizard allows you to select one of the five Telephony User Templates and change and define the user settings. The Telephony Template is stored in a file for use with the Add Users Wizard.

This template assumes you have already set up your lines and line pools. If this is not the case, refer to “Configuring Lines, Loops, and Routes” on page 91.

Refer to the next section for a description of the information required by this Wizard.

What You Need to Know

Before you fill out a template, look at the following list and determine what entries you want to include in the template. Detailed explanations of the fields can be found in this chapter.

Screen 1, Edit Template	
• Do you want to edit an existing template?	(Template <1 to 5> - <name>)
Screen 2, Template Name	
• Find a name that provides a descriptive clue as to what the template contains.	(Template Name)
Screen 3, CallPilot Voice Messaging	
• Do you want to add a new voicemail mailbox for the set?	No Yes
If yes . . .	
• Do you want to put this telephone into the Auto Attendant directory?	(In directory?) No Yes
• How do you want the telephone to dial out to voicemail?	Pool Line Route None
Screen 4, Line Assignment Refer to "Configuring Line Settings" on page 91.	
• Which lines do you want this telephone to have access to?	(Line) (enter line number) Add
Screen 5, Line Pool Access Refer to "Configuring Line Settings" on page 91.	
• Which line pools do you want this telephone to have access to?	(Pool) (enter line pool name) Add
Screen 6, Capabilities	
• Do you want a second call to ring if the telephone is busy?	(DND on busy) No Yes
• How do you want the handsfree feature to be activated?	(Handsfree) Auto None Standard
• Do you want to be able to answer a voice call without lifting the receiver or pressing the handsfree button on the telephone?	(HF Answerback) No Yes
• Do you want to include this telephone into a pickup group?	(Pickup group) None Group: 1 2 3 4 5 6 7 8 9
• What Page zone do you want this telephone to be in?	(Page zone) None Zone: 1 2 3 4 5 6
• Do you want to allow the user of this telephone to access the Paging feature?	(Paging) No Yes

• Which telephone, if any, do you want the telephone to dial when the direct dial number is entered on this telephone?	(Direct dial) None Set: 1 2 3 4 5
• Do you want the user to be able to use the Priority call feature?	(Priority Call) No Yes
• Do you want this telephone to have access to an auxiliary ringer?	(Aux ringer) No Yes
• Do you want to allow the user access to the Line Redirect feature?	(Allow redirect) No Yes
• Do want the user of the telephone to be able to redirect a ring?	(Redirect ring) No Yes

Screen 7, Call Forward

• If the call is not answered, where do you want to forward it to? (i.e. voicemail DN)	(Forward no answer to)
• How long do you want forward to delay on a call that is not answered? Note: This field appears after you enter a Forward no answer to DN.	(Forward no answer delay) 2 3 4 6 10
• If the telephone is busy, where do you want to forward the call? (i.e. voicemail DN)	(Forward on busy to)
• CallPilot Messaging DN	<DN number> (read-only)
• Do you want the telephone to have access to a Hotline number?	(Type) None Internal External
If internal . . . • What is the internal number for the hotline?	(Internal #)
If external . . . • What route are do you want the telephone to use to access the external number?	(Facility) Use prime line Use routing table Use <assigned line> <assigned line pool>
• What is the external number for the hotline?	External #

Using the Edit Template Wizard

After you have filled out the information in the previous section, follow these steps to run the wizard:

1. From the Programming Wizards page, enter the system user ID and password, then click the **Edit Template** button.

   If you do not know how to access the Programming Wizards page, refer to "Accessing the Wizards" on page 60.

2. Enter the information based on the choices you made in "What You Need to Know" on page 141.

3. The last page provides a summary of the information you chose. If you need to make changes, you must exit from the Edit Template Wizard, then start a new session.

4. Click the **Apply** button.

5. To use a template, refer to "Creating Telephone Records with the Add Users Wizard" on page 143.

Creating Telephone Records with the Add Users Wizard

Use the Add Users Wizard to change the telephony settings:

- for a range of DNs
- for a single DN

All the DN feature information can be entered when you run this Wizard, or you can indicate a pre-defined template that automatically sets up the DN features.

To determine what you need to enter for the DNs, refer to "What You Need to Know About the User" on page 144.

What You Need to Know About the User

Before you fill out the Add Users Wizard, use this list to determine what settings you want to include for the telephone.

Screen 1, Add Users	
• How many user sets do you want to configure? Select a single DN, a range of DNs, or several DNs scattered across the list.	(Choose one or more DNs)
• Do you want to use this wizard to define settings or use a preconfigured template?	(Use settings) Defined in this wizard From a pre-defined Template
If from template . . . • Which template do you want to choose?	(Template) Template <1 to 5> - <template name>
Screen 2, Per-DN settings	
• Enter the Name for each DN you are configuring.	(Template Name)
• If you want to create a target line, click the **Show Target Lines** link and fill out the line information.	Target line fields: (Line, Public #, Appr type, Appearances)
Note: The following fields do not need to be changed if you applied a template on Screen 1.	
Screen 3, CallPilotVoice Messaging	
• Do you want to add a subscribe mailbox for the DNs you are defining?	(Enable voicemail?) No Yes
If yes . . .	
• Do you want to put this telephone into the Auto Attendant directory?	(In directory?) No Yes
• How do you want the telephone to dial out to voicemail?	Pool Line Route None
Screen 4, Line Assignment Refer to “Configuring Line Settings” on page 91.	
• Which lines do you want this telephone to have access to?	(Line) (enter line number) Add
Screen 5, Line Pool Access Refer to “Configuring Line Settings” on page 91.	
• Which line pools do you want this telephone to have access to?	(Pool) (enter line pool name) Add

Screen 6, Capabilities	
• Do you want a second call to ring if the telephone is busy?	(DND on busy) No Yes
• How do you want the handsfree feature to be activated?	(Handsfree) Auto None Standard
• Do you want to be able to answer a call without lifting the receiver or pressing handsfree on the telephone?	(HF Answerback) No Yes
• Do you want to include this telephone into a pickup group?	(Pickup group) None Group: 1 2 3 4 5 6 7 8 9
• What Page zone do you want this telephone to be in?	(Page zone) None Zone: 1 23456
• Do you want to allow the user of this telephone to access the Paging feature?	(Paging) No Yes
• Which telephone, if any, do you want the telephone to dial when the direct dial number is entered on this telephone?	(Direct dial) None Set: 1 2 3 4 5
• Do you want the user to be able to use the Priority call feature?	(Priority Call) No Yes
• Do you want this telephone to have access to an auxiliary ringer?	(Aux ringer) No Yes
• Do you want to allow the user access to the Line Redirect feature?	(Allow redirect) No Yes
• Do want the user to be able to redirect a ring?	(Redirect ring) No Yes

Screen 7, Call Forward	
• If the call is not answered, where do you want to forward it to? (i.e. voicemail DN)	(Forward no answer to)
• How long do you want forward to delay on a call that is not answered? Note: This field appears after you enter a DN in Forward no answer to	(Forward no answer delay) 2 3 4 6 10
• If the telephone is busy, where do you want to forward the call? (i.e. voicemail DN)	(Forward on busy to)
• CallPilot Messaging DN	<DN number> (read-only)
• Do you want the telephone to have access to a Hotline number?	(Type) None Internal External
If internal . . . • What is the internal number for the hotline?	(Internal #)

If external . . .	
• What route are do you want the telephone to use to access the external number?	(Facility) Use prime line Use routing table Use <assigned line> <assigned line pool>
• What is the external number for the hotline?	External #

Using the Add Users Wizard

After you have filled out the information in the previous section, follow these steps to run the wizard:

1. From the Programming Wizards page, enter the system user ID and password, then click the **Add Users** button.
2. Proceed through the Wizard and add or change the information, based on what you entered in "What You Need to Know About the User" on page 144.
3. The last page provides a summary of the information you chose. If you need to make changes, use the **Back** button to navigate to the page where you need to make changes. Use the **Next** button to return to the **Summary** page when you have completed all your revisions.
4. Click the **Apply** button.
5. After you have configured the DNs, review each DN record and determine if you need to change any of the other settings. Refer to Figure 22 on page 147 to see what options are available, then refer to the detailed sections in this chapter and the following chapters to select the settings.

Note: Not all DN records have the same programming options. For example, ISDN sets do not have a **Button Programming** option.

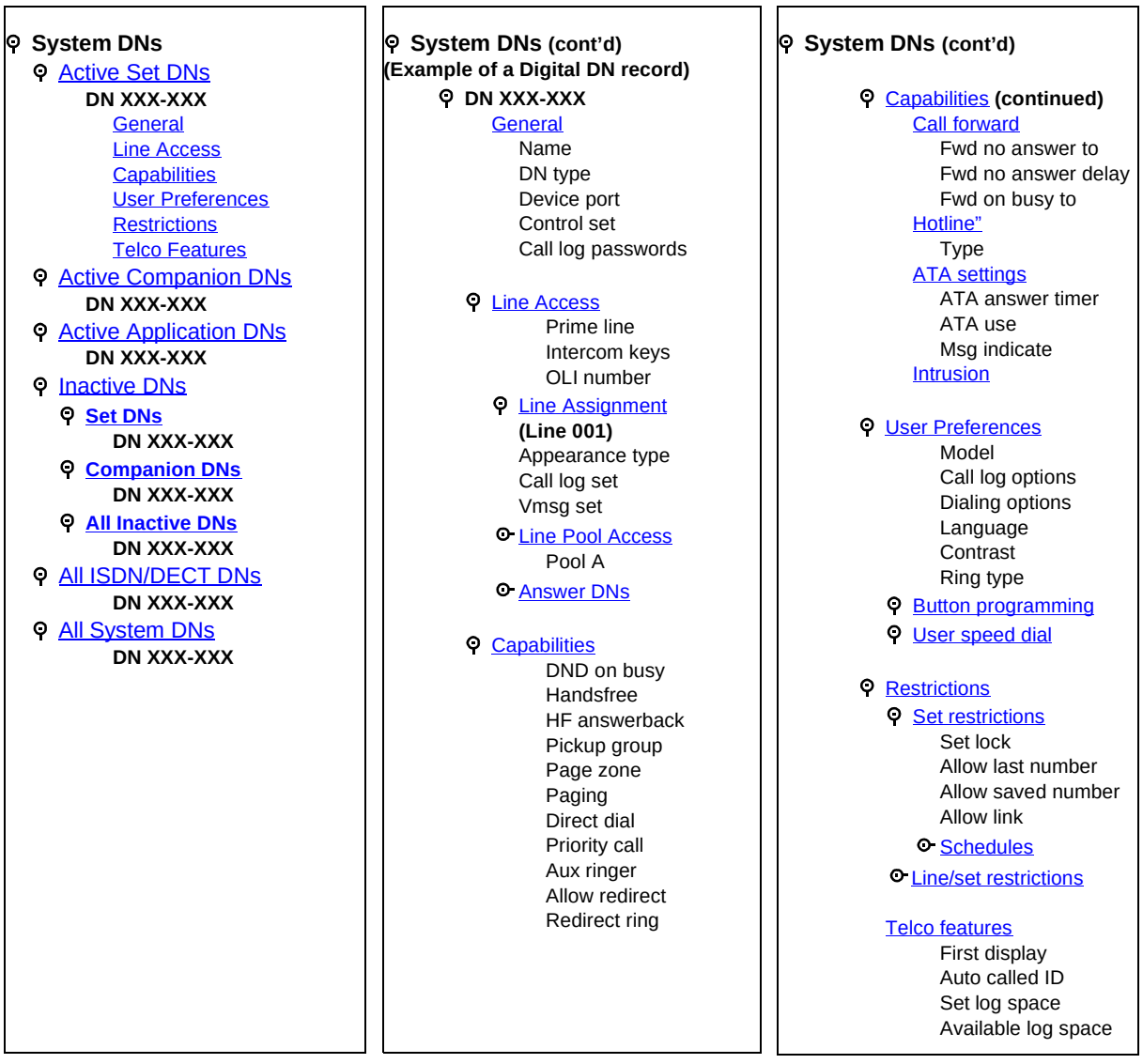
System DNs Headings and Features

Figure 22 shows a detailed view of the Unified Manager System DNs headings. The second two columns display the information found under a specific DN record number (DN XXX) regardless of which System DN second-level heading you access the record through.

Some features do not apply to some types of telephones. For instance, ISDN equipment cannot have button programming andATA settings apply only to analog telephones.

The headings shown for the DN record in Figure 22 are for a typical digital telephone.

Figure 22 DN headings and features



Copying Settings to Other DNs

The **Copy** command allows you to duplicate programming for a telephone and apply it to another telephone, a range of telephones, or to all the telephones on the system.

Note: Unique configurations, such as the name, do not copy over.

Follow these steps to copy telephone configurations:

1. Click on the keys beside **Services, Telephony Services, System DNs,** and **Active Set DNs**.
2. Click the telephone (DN 221-528) with the settings you want to copy.
3. On the **Edit** menu, click **Copy**.
4. Choose the data type you want to copy, **System data** or **System+user data**.
5. Click **Single, Range** or **All** from the Copy type list.
6. Type the DN number of the telephone or the range of sets (nnn-nnn) where you want to copy the settings. You do not have to fill in this box if you chose **All** in the Copy type list.
7. Click the **OK** button.

Identifying the Telephone (General Heading)

The **General** heading allows you to assign the name, the DN type, a control telephone, and a Call log password for a telephone. This record also shows you which physical port the telephone is accessing.

Follow these steps to identify a new telephone:

1. Click on the keys beside **Services**, **Telephony Services**, **System DNs**, and **Inactive DNs**.
2. Click on the key beside the heading that indicates the type of telephone you are installing.

   For example, click on the key beside **Set DNs** to program digital telephones or IP telephones.
3. Click the telephone record (**DN XXX**).
4. Click **General**.
5. Use the information in Table 31 to choose the general settings for the telephone.

Table 31 General record values

Attribute	Value	Description
Name	up to seven alphanumeric characters	Use this field to provide a more specific description of the telephone, such as the last name of the user or the location, or the actual extension number if it is different than the DN number.
DN type	Nortel digital set ISDN and DECT NA Portable	In the Business Communications Manager 2.5 software, the following defaults appear, based on the default DN settings: Nortel digital set: 221 (start DN) to 376 NA Portable (Companion): 565 to 596 ISDN and DECT: 597 to 624
		Note: ISDN and DECT and Companion DNs can be changed for either type of terminal if you require more DNs than what are presented for defaults.
Device port	<port number>	This number indicates the port number that this device is connected to, if the device is active, or which port the device would connect to, if the device is currently inactive. This field is not available or not shown for Companion and ISDN and DECT device records.
Control set	DN: <any telephone DN> None DN:221<start DN>	The Control telephone attribute allows you to define a DN that will act as a control telephone. A control telephone can turn Scheduled Services, such as Restriction Service on and off for the telephones assigned to it. For more information about services, see “Scheduled Services Headings” on page 249. You can assign several control sets for your system but you can only assign one control telephone per DN. * If you changed the Start DN, this number reflects that change.

Table 31 General record values (Continued)

Attribute	Value	Description
	TIPS: Control telephone • You must program external lines and telephones with a control telephone to use the Scheduled Services: Ringing, Restriction, and Routing Services. • Nortel Networks recommends that the control telephone you assign for all telephones (DNs) is different from the control telephone you assign for the lines. • You can turn on a service manually or automatically for all telephones controlled by a given control telephone, but you cannot combine schedules. In other words, a service can only be active as normal service or one of the six schedules at any one time.You can have several schedules active, as long as they are using different services.	
Call Log Password	<four-digit alphanumeric or blank>	Set the Call log password for the telephone. If a user forgets their password, you can reset it by leaving this box blank or entering a new password. The user can then enter a new password from their telephone.

Using the Line Access Heading

Line access allows you to assign lines or line pools to individual telephones.

You can copy settings to other telephones. If you are assigning the same lines to a number of sets, you can set up anTemplate with the Edit Template Wizard, and use the Add Users Wizard to assign the settings to a range of sets all at once. Refer to “Creating User Templates with the Edit Template Wizard” on page 140 and “Creating Telephone Records with the Add Users Wizard” on page 143.

Assigning Line Access

The prime line for a telephone is the line that is automatically selected when a call is made from the telephone.

The default for all telephones is:

- Prime line: I/C (intercom)
- Intercom keys: 2

If you want to change the prime line or intercom key settings, following these steps:

1. Choose the DN record you are assigning lines to.
2. Click on the **Line access** heading.

3 Use Table 32 to select the values for line access.

Table 32 Telephone line access fields.

Attribute	Values	Description
Prime line	None, Pool (A to O), I/C (intercom), Line: <line numer>	Choose the first line that the telephone selects when a call is made. PRI pools are not valid selections for a Prime line. When you assign a line pool as a prime line, the system searches automatically for an idle line in the pool. For related information, refer to "Rules About Assigning Prime Lines:" on page 151
Intercom (I/C) keys	0 to 8	Assign the number of intercom buttons to a telephone. Intercom buttons provide a telephone with access to internal and external lines, and line pools. Refer to "About Intercom (I/C) Keys" on page 152.
OLI number	<up to 24 digits (10 digits, North America)>	Define the originating line identification number (OLI) which appears on the telephone being called from this telephone. Refer to "Entering Originating Line Identification (OLI)" on page 152.

Note: ISDN terminals/DECT handsets

Prime lines and Intercom keys are not supported for these sets.

DECT handsets can only dial outside lines using access or destination codes.

Rules About Assigning Prime Lines:

Read the following before you assign Prime lines to a telephone.

- You must assign an external line to the telephone in **Line assignment** before you can assign the line as the prime line to the telephone. Refer to "Determining Line Assignments" on page 152.
- You must assign a line pool to the telephone in **Line pool access** before you can assign a line pool as the prime line to the telephone. Refer to "Assigning Line Pool Access" on page 155.
- A target line cannot be a prime line for a telephone because a target line is incoming-only.

Note: Do not assign a T1 DID line as the prime line for a telephone. If assigned, the system treats it as if there is no prime line. The telephone displays the message **Select a line** when you lift the receiver.

- PRI lines are set to Auto Answer. You cannot change a PRI line to Manual Answer.
- When you assign line access for BRI loops, make sure that the programming for the two lines on the BRI T1 or PRI loop is identical. For example, if line 001 on BRI loop 201 appears on a DN, line 002 on the same loop must also appear on the DN.
  In general, do not assign, auto-answer loop start trunks and auto-answer BRI trunks to telephones. If assigned, use these trunks to monitor incoming call usage, or to make outgoing calls.

About Intercom (I/C) Keys

The Intercom keys attribute assigns the number of intercom keys. Intercom keys provide access to internal and external lines and line pools. The user uses the intercom key to answer internal calls, or to select a line or line pool to make a call.

When you assign each Intercom key during programming, it automatically appears on the telephone. The intercom keys appear on the lower-right button, or one key above if the Handsfree/ Mute feature appears on the telephone.

When you assign the number of Intercom keys the following occurs:

- A telephone requires two Intercom keys to establish a conference call with two other Business Communications Manager telephones.
- You require only one intercom key if the button is used to make and receive internal calls, and to access line pools. You require two intercom keys for a telephone with several lines assigned to Ring only.
- You can assign a maximum of eight intercom buttons to the T7100 telephone, even though the telephone has only one programmable button. However, you can use only two intercom buttons at one time.

Entering Originating Line Identification (OLI)

The originating line identification (OLI) number setting allows you to specify the number that displays on the telephone you are calling.

Enter the digits used for the OLI number. When you make an outgoing call on a BRI line, the Call Display information that appears on the telephone you are calling is usually based on the first Network DN associated with the line.

If the line has more than one Network DN, you can program a DN to use a Network DN other than the first DN for the outgoing Call Display information. When you program the alternate Network DN as the ten-digit OLI number, and you make a call using the line associated with the Network DN, the OLI number appears on the telephone you are calling.

If an outgoing call is made using a line that is not associated with the Network DN number used as the OLI number, the network ignores the number. In this case, the default Call Display information appears, which is the first or only Network DN associated with the line.

Determining Line Assignments

The Line assignment setting allows you to assign physical trunks and target lines to each telephone.

Applying Target Lines

You can assign and remove target lines in the same way as for other lines.

You can also assign multiple target lines across a group of sets in a Broadcast hunt group.

Assigning Outgoing Lines

Follow these steps to assign outgoing lines:

1. If you are not already in the DN record, click the telephone DN to which you want to assign a trunk or line.
2. Choose **Line access**. Click on the **Line assignment** heading.
3. Click the **Add** button.
4. Type a line number in the **Line** box.
5. Click the **Save** button.
6. On the navigation tree, click the **Line nnn** you just created.
7. Use Table 33 to define the line for the telephone.

Table 33 Telephone line assignment fields

Attribute	Values	Description
Appearance type	Ring only, Appear & Ring, Appear only	Select how a call on this line shows on the telephone. If you choose **Appear&Ring** or **Appear only**, you can have as many simultaneous DID calls as there are target line key appearances. If you choose **Ring only**, you can have as many simultaneous DID calls as you have intercom keys.
		Note: The Business Communications Manager does not support a mixture of **Appear only** and **Ring only** appearances for the same line.
Appearances (for target lines, only)	<digit>	Selects the number of appearances of a target line.
Call log set	Y or N	Specify whether the telephone automatically logs Call Display information for calls on an external line. The line must appear on that telephone, but it does not have to be a ringing line.
Vmsg set	Y or N	Select whether an indicator shows on the telephone for voice message waiting to an external voice message system. The line must appear on receiving telephone.
		Note: Contact your voice message service provider, to find out if your voice message service works with Business Communications Manager, or if you have any problems with your service.

Caution: PRI Lines

Users cannot access PRI lines directly through line appearances or line pools. To dial outgoing PRI calls use the intercom button and enter a routing code.

If you change a digital trunk module (DTM) to PRI, the system automatically removes all existing line appearances for that module.

Note: ISDN terminals/DECT handsets

Call log set and Vmsg set are not supported for these telephones.

Notes about Assigning Lines to Telephones

Read these notes for more information about assigning lines to telephones.

- The Business Communications Manager Analog Terminal Adapter (ATA 2), BRI S-terminals, or a portable telephone cannot process more than two simultaneous calls.
- Nortel Networks recommends a maximum of four line buttons per telephone. You can program more than four line buttons on a telephone by programming less than four on other sets. For example, you might program 20 line buttons on a receptionist telephone equipped with a CAP and only two lines on all other telephones.
- Do not assign auto-answer loop start trunks, auto-answer T1 E&M trunks and T1 DID trunks to telephones. If assigned, use them to monitor incoming call usage, or make outgoing calls (auto-answer loop start and T1 E&M trunks).
- You cannot assign a line that is private to another telephone.
- Each line assigned to appear at a telephone must appear at a button with an indicator on that telephone. The maximum number of line buttons is eight for the T7208 telephone, 10 for the T7310 telephone, and 24 for the M7324 telephone. However, you need to also consider other button requirements such as intercom keys and a mute/handsfree key.
- If you set a line to Ring only, incoming calls appear on an intercom button.
  A central answering position (CAP), with one or two CAP modules, can provide extra line buttons if more than 24 lines are assigned to the CAP. The remaining lines appear on buttons on the CAP module.

  The T7100 telephone is an exception; it has no line buttons and you can assign any number of lines. Assign the lines on an T7100 telephone to ring; otherwise, you cannot detect incoming calls on the lines.

Assigning Line Pool Access

The Line pool access heading allows you to define the line pools that the telephone will be able to access for outgoing calls. These shared pools of lines allow many users to use fewer lines for connections where dedicated lines are not practical or not desirable. If all lines in the pool are taken, the user receives a busy signal.

To assign a line pool to a telephone:

1. If you are not already in the DN record, click the telephone DN to which you want to assign a line pool.
2. Click **Line access**, then click **Line pool access.**
3. Click the **Add** button.
4. Enter a line pool identifier. <a letter from **A** to **O,** inclusive>.
5. Click the **Save** button.

   The line pool identifier appears under the Line pool access heading.

About PRI Line Pools

PRI lines have special requirements when being used within line pools.

- Six exclusive line pools (PRI-A to PRI-F) are available for PRI lines. The system currently supports only three line pools.
- Only PRI or BRI ETSI QSIG lines can belong to a PRI pool.
- PRI lines cannot belong to Line Pools A through O.
- All lines on a single DTM (PRI) belong to the same pool. Lines from multiple DTM (PRI) can belong to the same pool if they are configured with the same protocol.
- You can assign PRI lines to pools with the **Line type** setting.

Using Answer DNs

You can program a telephone to provide automatic call alerting and call answering for other telephones in the system. The DNs of the other telephones are referred to as Answer DNs.

Every Answer DN you assign to the telephone automatically designates an appearance on the answer telephone beside a button that can be used to answer. On the answer telephone, an indicator beside the answer button lights when a call comes in from the original telephone. Label the buttons to identify the telephone with its name or DN. More than one telephone can have an Answer button for the same DN.

You can assign a maximum number of eight Answer DNs to a telephone.

Mobility sets: For Companion and DECT telephones, you can twin desk sets with the portable sets by assigning the Companion or DECT portable DNs to a desk telephone Answer DN. Companion and DECT portable handsets do not have answer buttons, so you can only assign one originating telephone to each telephone. If you want to share a portable telephone among users, use the Call Forward feature to temporarily call forward a desk telephone DN to the portable handset.

Warning: DECT security notice.

Ensure that your DECT handset is set to answer calls manually. Otherwise, if a call is forwarded to the handset with appearance only, the handset will answer the call with no indication to the user that the line is open.

Assigning Answer DNs

Use these steps to assign Answer DNs to a telephone:

1. If you are not already in the DN record, click the telephone DN to which you want to assign an answer DN.
2. Choose **Line access**.
3. Click on the **Answer DNs** heading.
4. Click the **Add** button.
5. Type the answer DN.
6. Click the **Save** button.
7. On the navigation tree, click Answer **DN**.
8. Use the information in Table 34 to configure the line appearance.

Table 34 Answer DN settings

Attribute	Values	Description
Appearance type	Appr & ring Appr only	Choose how you want the line to notify the answer telephone that a call is coming through. Appr & ring: The call number will display and the telephone will ring Appr only: The call number will display, but there will be no ring

Defining Capabilities

The **Capabilities** headings control how the system interacts with individual telephones, and how the telephones receive calls.

Use these steps to define capabilities for a telephone.

1. If you are not already in the DN record, click the telephone DN to which you want to assign set capabilities.
2. Click the **Capabilities** heading.
3. Use the information in Table 35 to configure the telephone capabilities.

Table 35 Capabilities fields

Attribute	Values	Description
DND on busy	Y or N	Defines whether an incoming call rings if you are already on another call.
Handsfree	Auto Standard None	**None**: The handsfree feature is not available to this telephone. **Standard**: The handsfree feature is activated by pressing a button on the telephone. **Auto**: The handsfree feature is activated when the telephone receives a call.
HF answerback	Y or N	Defines whether you can automatically answer a voice call without lifting the receiver or pressing the Handsfree/Mute button.
Pickup group	None 1 to 9	Assigns this telephone to a pickup group. This is a group where all sets ring until one is answered.
Page zone	None 1 to 6	Assigns this telephone to a page zone.
Paging	Y or N	Defines whether you can make paging announcements from this telephone.
Direct dial	Set 1 to Set 5 None	Defines whether you can call the Direct-dial telephone from this telephone using the Direct-dial digit.
Priority call	Y or N	Defines whether this telephone can interrupt calls or override Do Not Disturb at another telephone.
Auto hold	Y or N	This setting determines if the system will automatically put an active call on hold if you answer or initiate another call. If you choose No, the system will drop the active call if you answer or initiate another call, unless you press the [ ] button. The user can change the Auto Hold setting using [ ] 7 3 on the telephone. **Administrators please note:** This user feature code is not yet noted in the *Telephone Feature Programming Guide* or on the Telephone user cards.
Aux ringer	Y or N	Defines whether an auxiliary ringer (if installed) rings for incoming calls at this telephone.

Table 35 Capabilities fields (Continued)

Attribute	Values	Description
Allow redirect	Y or N	Defines whether the line to this telephone can be redirected. This must be set to Y to allow call forwarding outside the network (external call forward).
Redirect ring	Y or N	Defines whether the telephone rings briefly when a call on one of its lines is redirected by the Line Redirection feature (8 4).

Note: ISDN terminals/ DECT handsets
- DND on busy is not supported.
- Handsfree is supported. For DECT handsets, leave the setting at AUTO.
- HF answerback is not supported.
- Pickup group is not supported.
- Direct dial is not supported.
- Priority call is not supported.
- Allow redirect and Redirect ring are not supported.

Assigning Call Forward

The **Call Forward** setting allows you to defines how the system handles calls when the call is unanswered or the line is busy.

You can enter internal numbers, external numbers, and routing codes to process these calls. For instance, if your voice mail system is on a Meridian system, you would call forward unanswered calls to that number. The number you enter must include access codes, if required for network access.

Use these steps to set up the Call Forward feature on a telephone.

1. If you are not already in the DN record, click the telephone DN to which you want to assign Call Forward properties.
2. Click on **Capabilities**.
3. Click on **Call forward**.
4. Use the information in Table 36 to configure the call forward settings.

Table 36 Call forward fields

Attribute	Values	Description
Fwd no answer to	up to 24 digits	Enter the number to which you want to redirect unanswered incoming calls.
Fwd no answer delay	2, 3, 4, 6, 10	Define the number of rings before the system forwards an unanswered call. This heading only appears after you have entered a Call Forward No Answer number and pressed Enter.
Fwd on busy to	up to 24 digits	Redirect incoming calls when this telephone is busy with another call.

Assigning a Hotline

The Hotline heading allows you to define a telephone number that automatically dials when you lift the receiver or press the Handsfree/Mute button on a telephone.

Use these steps to define an internal or external Hotline number.

1 If you are not already in the DN record, click the telephone DN to which you want to assign a hotline.

2 Click on **Capabilities**.

3 Click on **Hotline**.

4 Use Table 37 to configure the hotline setting for a telephone.

Table 37 Hotline values

Attribute	Values	Description
None		The telephone does not automatically dial any number.
Internal	Internal # Direct dial set DN:	Define the internal telephone you want to access. Direct dial set: Will automatically dial a telephone on the system defined as a direct dial telephone DN: the DN of the telephone that gets automatically dialed when the user picks up the handset
External	External # **Facility Value:** Use line nnn Use prime line Pool code Use routing table	Enter the complete call number for the external telephone you want to access. Enter the line you want the call to use. (This cannot be a target line.) **Use line nnn**: Refer to line assignment for this telephone. **Use prime line**: Refer to the General record for this telephone. **Pool code**: Refer to the line pool assignment for this telephone. **Use routing table**: Refer to the routing tables. The destination code for that table must be part of the External #.

Note: ISDN terminals/DECT handsets

This feature is not supported for this equipment.

Determining ATA Settings (Analog Telephones)

The Analog Terminal Adapter (ATA) settings allow you to define general settings for analog terminal adapters. These settings apply to analog DNs only and are available to telephone DNs in the digital telephone range only.

Follow these steps to configure the ATA settings:

1. If you are not already in the DN record, click the telephone DN to which you want to assign ATA settings to.
2. Click on **Capabilities**.
3. Click on **ATA settings**.
4. Use the information in Table 38 to configure ATA settings.

Table 38 ATA settings

Attribute	Values	Description
ATA answer timer	3, 5, 7, 10	Select the length of delay between the last digit you dial and when the ATA 2 device is ready to receive DTMF tone.
ATA use	On site Off site	Select the location of theATA 2.
Msg Indicate	None Tone Lamp	Tone sends a Message Tone through the telephone receiver when you receive a message. Lamp turns on the Message Lamp when you receive a message.

Tips: If you have a modem or fax machine, keep theATA answer timer delay short. If a call to a fax machine or modem cannot connect, shorten the delay. If an individual dials the number for a fax machine or modem, make the delay a little longer.

Setting Intrusion Controls

If break-in feature is allowed on any MCDN lines assigned to the telephone, you need to define the level of untrusion for each telephone. This determines if the user can use the feature, and to what degree.

Follow these steps to set Intrusion levels.

1. If you are not already in the DN record, click the telephone DN to which you want to set an intrusion level.
2. Choose **Capabilities**.
3. Click **Intrusion**.
4. In the **Protect lvl** field choose an access level.

   There are four levels of access:

   - None — feature is turned off, user cannot break in on any calls
   - Low — user can only break into calls on other telephones with low level protection
   - Med(ium) — user can break into calls on other telephones with low and medium-level protection
   - High — user can break into calls on all other telephones with this feature

Defining User Preferences

The User preferences headings allow you to program the same settings that users can do at their telephones. These options are only available to sets that display Nortel Digital Set on the **General** record of the DN record. For instance, ISDN and DECT or Companion sets do not have user preferences. Programming performed by users at their own sets, takes precedence over these settings. User telephone programming is described in the *Telephone Features Programming Guide*.

Use these steps to program user preferences for a telephone.

1. If you are not already in the DN record, click the telephone DN to which you want to assign a user preferences.
2. Click the **User preferences** heading.
3. Use the information in Table 39 to configure user preferences.

Table 39 User preference choices

Setting	Values	Description
Model	Other M7100 M7208 M7310 M7324 i20XX i2002 IPWIs DECT	If you have not yet attached a telephone, choose the model of the telephone. This will create a number of defaults based on the telephone capabilities. • You cannot change the model if the telephone is already attached. • ISDN and NA Portable sets are designated as Other. • Equivalents for Business Series Terminals: M7100 = T7100; M7208 = T7208; M7310 = T7316 • i20xx refers to i2004 and i2050 sets
Call log options	Log all calls, No autologging, No one answered Unanswered by me	Select how you want the telephone to handle logging calls. **Log all calls**: All calls are noted in the call log. **No autologging**: No calls are automatically logged. **No one answered**: Unanswered calls are not logged. **Unanswered by me**: Unanswered calls are not logged.
Dialing options	Standard dial pre-dial automatic dial	Select how you want the telephone to handling information you dial into it.
Language	Languages displayed are based on telephone capabilities and system software	Choose the language for the telephone display prompts.
Contrast	1, 2, 3,4, 5.....9	Adjust the contrast of the display.
Distinct rings in use	read only	This field indicates the distinct ring patterns are currently in effect, if any, on any lines, telephones, or hunt groups on the system.

Table 39 User preference choices (Continued)

Setting	Values	Description
Ring type	1, 2, 3, 4	Select a ring pattern for the set. Default is 1.
	Warning: If you assign a distincitive ring pattern to a telephone, and that distincitve ring pattern has already been assigned to a line, all lines with that ring pattern will be reset to None. If you assign a distinctive ring pattern to a line, and that distinctive ring pattern has already been assigned to a telephone, all telephones with that ring pattern will be reset to pattern 1. Refer to "Distinct ring" on page 99.	

Programming Telephone Buttons

Button programming allows you to program the buttons on a telephone with internal and external autodialers and with programmed feature keys. Button programming is only available on digital and IP telephones supported by the Business Communications Manager. ISDN terminals, Companion and DECT portable systems do not have programmable buttons.

To view a list of the available feature selections, refer to Appendix , "Button programming: Features," on page 593. For detailed descriptions of the features and how to program them either with the Unified Manager or from the telephone, refer to the *Business Communications Manager 2.5 Telephone Features* Programming Guide.

Follow these steps to program the buttons on a telephone.

1. If you are not already in the DN record, click the telephone DN where you want to program button features.
2. Click the key to expand the **User preferences** heading.
3. Click the **Button programming** heading. The list of available buttons appears.
4. Click the button number that you want to program.
5. Use the information in Table 40 to configure button preferences.

Table 40 Button programming choices

Setting	Values	Description
External autodial	<external phone number> Use prime line Pool <line pool code> Use routing table Use line <line number>	Enter the number the telephone will automatically dial when this button is pushed. You also need to choose the route the telephone will dial through. **Prime line**: the prime line assigned to the telephone **Pool X**: one of the pools assigned to the telephone **Routing table**: enter the destination code with the external phone number **Use line X**: one of the lines assigned to the telephone

Table 40 Button programming choices (Continued)

Setting	Values	Description
Feature	<feature name>	Choose the feature you want to invoke when this button is pushed.
Blank		The button has no feature settings.
Internal autodial	<Internal DN>	Enter the DN number for the internal telephone you want the telephone to ring from this button.

Caution: Replacing telephones.

If you unplug a telephone, the Business Communications Manager will retain the programming for that DN on two conditions:

- The original telephone is replaced with the same model.
- The original telephone is plugged in somewhere else on the system before any other telephone is plugged into the jack from which the telephone was removed.

Assigning User Speed Dials

Speed dial numbers allow users to dial out a number with one button press. The number of speed dial entries that a user can have on a telephone depends on the number of physically-available feature buttons on the telephone.

Follow these steps to set up speed dial numbers for individual telephones.

1. If you are not already in the DN record, click the telephone DN for which you want to assign user speed dial numbers.
2. Click the key to expand the **User preferences** heading.
3. Click the **User speed dial** heading.
4. Click the **Add** button above the navigation tree. The Add User speed dials screen appears.
5. In the **Speed dial #** box, type in the code from 71 to 94 to assign the speed dial code.
6. Click **Save**.
7. Click the **Speed Dial # XX** heading you want to program.

   A DN XXX Speed Dial # XX screen appears.

8 Use the information in Table 41 to set the speed dial number and route for the speed dial code.

Table 41 User speed dial settings

Setting	Values	Description
External #	<external phone number>	Enter the number the telephone will automatically dial when this code is entered. Remember to include the access codes for the route you choose.
Facility	Use prime line Use line 001 Pool A Pool M Use routing table	Choose the route for the number to dial out.

Programming Restrictions

The Restrictions settings prevent callers from making certain kinds of calls from a specific telephone or from lines that are available at the telephone. You can also restrict some features.

You can copy the restriction settings you program on one telephone to other telephones.

Defining Set Restrictions

The Set restrictions screen allows you to assign a restriction filter to a telephone to prevent certain numbers from being dialed from that telephone and prevent the use of certain features.

Follow these steps to create or change set restrictions:

1 If you are not already in the DN record, click the telephone DN for which you want to assign set restrictions.

2 Choose **Restrictions**.

3 Click **Set restrictions**.

4 Use the information in Table 42 on page 166 to configure telephone restrictions.

Table 42 Telephone restriction fields

Setting	Values	Description
Set lock	None Partial Full	Choose the option that sets the amount of programming and customizing the user can do with this telephone. **None** allows access to all features.
		Partial prevents: • programming autodial buttons • programming user speed dial numbers • programming feature buttons • moving line buttons • changing the display language • changing dialing modes (Automatic, Pre-, and Standard Dial) • using Voice Call Deny • saving a number with Saved Number Redial
		Full restricts all the Partial settings, plus: • changing Background Music • changing Privacy • changing Do Not Disturb • using Ring Again • using Call Forward all calls • using Send Message • using Trunk Answer • activating Services
Allow last number	Y or N	Allows or disallows access to the Last Number Redial feature.
Allow saved number	Y or N	Allows or disallows access to the Saved Number Redial feature.
Allow link	Y or N	Allows or disallows access to the Link feature, which is a host signaling option.

Note: ISDN terminals/DECT handsets

- Set lock is not supported.
- Allowed last number redial is supported on some sets. Refer to the user manual for your telephone.
- Allowed saved number redial is not supported
- Allow link is supported on some sets. Refer to the user manual for your telephone.

Setting Restriction Schedules for Telephones

You can assign a different restriction filter for normal service and for each of six other schedules. See "Scheduled Services Headings" on page 249 for more information about the schedules.

Follow these steps to configure Set Restriction Schedules:

1. If you are not already in the DN record, click the telephone DN for which you want to assign set restrictions schedules.
2. Click the telephone (DN 221-528).
3. Choose **Restrictions, Set restrictions, Schedules**.
4. Click the schedule you want to program. For example, **Evening**.
5. In the **Use filter** box, type in the number of the restriction filter you want to assign to the telephone. Refer to Figure 43.

Table 43 Schedule filter defaults

Schedule	Restriction filter (defaults)
Normal	02
Schedule 1 (Night)	11
Schedule 2 (Evening)	12
Schedule 3 (Lunch)	13
Schedule 4	00
Schedule 5	00
Schedule 6	00

For example, if you enter a set of restrictions for filter 11, the restrictions will automatically apply for the Night schedule.

Defining Line/set Restrictions

The **Line/set restrictions** settings allow you to assign a restriction filter to a specific line for outgoing calls at a specific telephone. This type of filter replaces any line or set restriction filters that can otherwise apply. Line/set restrictions restrict the numbers the user can dial on a line, but only from that telephone. The same line on another telephone can have different restrictions.

You can apply a different line restriction for normal service and for each of six schedules.

Follow these steps to configure Line/set restrictions settings:

1. If you are not already in the DN record, click the telephone DN for which you want to assign line/set restrictions.
2. Choose **Restrictions/Line/set restrictions.**
3. Click the **Line** number you want to configure.

   The list of schedules expands on the navigation tree.
4. Click the schedule name that you want to configure. For example, **Night**.

   The Night schedule window appears.
5. In the **Use filter** box, choose **None** or **Filter:**

   Type the number you want to assign as the Line/set restriction for this schedule and press the **Enter** key. There are no default Line/set restrictions.

Tips: You can apply a maximum of 255 line/set restrictions to lines at telephones.
If you assign a Line/set restriction to a line at a particular telephone, it overrides any line restrictions or telephone restrictions that might otherwise apply.
If no Line/set restrictions are defined, the system checks the numbers dialed against the telephone restrictions and the line restrictions, if either of these are defined.
The numbers dialed can be rejected by either restriction.

Configuring Telco Features

The Telco features heading allows you to program how the Business Communications Manager works with the public network or other outside features and services. Business Communications Manager works with two of these services: Call Display and an external voice message service.

You can copy the Telco features settings you program on one telephone to other telephones.

Follow these steps to configure Telco features settings:

1. If you are not already in the DN record, click the telephone **DN** for which you want to assign telco features.
2. Click on **Telco features**.
3. Use the information in Table 44 to configure Telco features.

Table 44 Telco features settings

Setting	Values	Description
Feature assignment	<line number>	If you subscribe to Call Display services, external calls are identified on the display. A message indicator from an external voice mail service can also show on the telephone display. Analog Call Display services are available with a CTM. PRI also provides the Caller ID. You can customize how this information is used.
First display	Name Number Line	Determine what call display information appears first. This feature depends on what services you subscribe to. Call Display information may contain the name of the caller, the number of the caller, the name of the line in your Business Communications Manager system that the call is on, or all. For each telephone, you can determine what information displays first.
	Tips: The Call Information feature displays and toggles between the name and line number for Call Display information. Unknown number appears on the display if the information is not available from your telephone company. You may see Private number on the display if the caller blocks that information.	
Auto called ID	Y or N	Select whether you want to see the extension number and name of the telephone you call on your display. The Auto called ID set for target lines is the same telephone that has appearance on that target line.
Set log space (read-only)	<amount of space remaining on the log>	The Log space setting determines the number of items that can be stored in the Call log for each telephone. There is no log space assigned by default.

Note: DECT handsets

DECT handsets display numbers for incoming calls from outside the local network, and displays the telephone name for incoming calls from internal sets.

Digital Telephones DN Record Matrices

Transfer the following information to a spreadsheet and fill out the values for each telephone you provision.

Table 45 DN equipment identification

Name or location	DN type	BLF	CAP	ATA	Port No.	Default DN (max. 7 digits)
Control set (default is start DN						
Call log passwords						

Table 46 General and Line access settings for DNs

Sets: (max. 7 digits)			
Prime Line	None I/C Line # __ Pool ____	Line pool access	PRI-A PRI-B A B C D E F G H I J K L M N O
Intercom Keys	0 1 2 3 4 5 6 7 8	Answer DNs Enter DNs of sets to be answered and circle Answer DN type. AR = Appear&Ring A = Appear only blank = Unassigned	A R A R A R A R
OLI#	None #		
Line assignment List three- digit line number and circle line assignment. AR = Appear&Ring A = Appear only R = Ring only blank = Unassigned	001 A R 002 A R _ _ _ A R _ _ _ A R _ _ _ A R _ _ _ A R _ _ _ A R		
Call log set	Y N		
Vmsg set	Y N		

Table 47 Capabilities

Sets: (max. 7 digits)	
Capabilities screen	
DND on Busy	Y N
Handsfree	Auto Std None
HF answerback	Y N
Pickup grp	1 2 3 4 5 6 7 8 9 None
Page zone	1 2 3 4 5 6 None
Paging	Y N

D-Dial	Set1Set __ None
Priority call	Y N
Aux. ringer	Y N
Allow redirect	Y N
Redirect ring	Y N

Call Forward	
Fwd no answer	None to:
Fwd delay	2 3 4 6 10
Fwd on busy	None to:
Hotline	
None	
Internal	Internal #
External	Facility Prime Pool A Use Routing Table External #

ATA settings	
ATA answer timer	3 5 7 10
ATA use	On site Off site
Msg indicate	None Tone Lamp
Intrusion	
Protect lvl	None Low Med High

Table 48 User preferences

Sets: (max. 7 digits)				
Model	M7324 M7310 (T7316) M7208 (T7208) M7100 (T7100) Other: CAP ATA Intl set Companion		Call log opt'ns	Log all calls... No autologging... No one answered... Unanswered by me...
Dialing opt'ns	Standard dial Pre-dial Automatic dial		Display cntrst	1 2 3 4 5 6 7 8 9
Language			Ring type	1 2 3 4

Table 49 Button programming

Model				
Button number	Blank	External Autodial	Internal Autodial	Feature
		External #: Use Line: Use Prime Line Use Pool Use Routing Table	DN DN:	

Table 50 User speed dial settings

Spd# (71-94)	**Speed dial number (max. 24 digits)**	Use prime line Use line: ____	Pool code ____ Use routing table

Table 51 Telephone (set) Restrictions

Restrn flt	Restrn		Default Overrides	
	(Number)	(Value)	(Number)	(Value)
00		No restrictions (only filter that cannot be changed)		
01	01	0		
	02	1	001	1800
			002	1877
			003	1888
	03	911	001	911

Table 51 Telephone (set) Restrictions (Continued)

	04	411		
	05	976		
	06	1976		
	07	1•••976		
	08	1900		
	09	1•••900		
	10	5551212		
02-99 . . .				
Restrn flt	Restrn nn		Override	
(01-99)	# (2digits)	Restriction (max. 15 digits)	# (3 digits)	Overrides (max. 16 digits)
Set lock	None Partial Full			
Allow last number	Y N			
Allow saved number	Y N			
Allow link	Y N			

Table 52 Telephone restriction schedules and line/set restrictions

Sets: (max. 7 digits)				
Names (max. 7 char.)				
Set restriction schedules			Line/set restrictions	
Filters				
Normal	02	02,	Normal None	
Night	11	11,	Night None	
Evening	12	12,	Evening None	
Lunch	13	13,	Lunch None	
Sched 4	00	00,	Sched 4 None	
Sched 5	00	00,	Sched 5 None	
Sched 6	00	00,	Sched 6 None	

Table 53 DN record, Telco features

Sets: (max. 7 digits)			Auto Called ID	
names: (max. 7 char.)			Set log space	
First display	Name Number Line		Available log space	

Setting CAP Assignments

The CAP assignment setting designates a telephone as a Central Answering Position (CAP). The CAP must be an M7324 telephone, which may have one or two CAP modules attached. Any M7324 telephone in the system can be assigned up to two CAP modules. However, of those modules assigned as CAPs, a maximum of five modules can have lines assigned to them. These CAP modules are known as Enhanced CAPs (ECAP).

You can use CAPs to:

- monitor the busy/not busy and Do not disturb status of Business Communications Manager telephones
- answer external calls on up to 120 lines, and extend calls to other Business Communications Manager telephones
- send up to 30 messages to other Business Communications Manager telephones
- provide up to 96 extra memory buttons for the M7324 telephone

Note: If you do not require line appearances on a telephone, do not program the telephone as a CAP.

Configuring a CAP assignment

Follow these steps to create CAP assignments:

1. Click on the keys beside **Services**, **Telephony Services**, and **General Settings**
2. **Click on the key beside CAP assignment**.
3. Click the CAP you want to program (**CAP 1-CAP 5**).
   The CAP # window appears.
4. Type the DN of the M7324 telephone you want to designate as a CAP.

Tips: If CAP modules are attached to an M7324 telephone that has not been programmed as a CAP, then no CAP settings are assigned.
If a CAP module (or modules) is relocated with the M7324 telephone, the settings are retained.

Chapter 8
Controlling Access to the System

This chapter describes the telephony configurations that are used to control access to the system or system features.

DN Lengths

The DN lengths setting allows you to change the number of digits for the Received number length and the DN length.

Warning: Do not change DN length immediately after a system startup.
You must wait for at least two minutes after a system startup before you change the DN length. It is preferable that you change this setting at system startup using the Quick Start Wizard. Refer to "What You Need to Know" on page 63.

If you change the DN length after startup:

- Data devices drop calls when you change the DN length during system operation. These data devices use the B2 channel. System telephones use the B1 channel. These telephones do not drop calls when you change the DN length.
- The DN length change takes up to two minutes, depending on the size of the Business Communications Manager system. System response can briefly slow down during this time.

Tips: Increasing the DN length

Each increase in length places the digit 2 in front of any existing DN. For example, if DN 234 was increased to a length of 4, the new DN would be 2234.

If the DN length change creates a conflict with the Park prefix, external line access code, direct-dial digit, or any line pool access code, the setting for the prefix or code changes to None, and the corresponding feature is disabled.

Warning: Voice mail and Call Center applications are reset if you change the DN length after these services are installed.

To change the DN length after startup, follow these steps:

1 Choose **Services**, **Telephony Services**, **General settings**

2 **Click on DN lengths**.

The DN lengths window appears in the right frame.

Table 54 lists the possible values that can be entered for DN length.

Table 54 DN length values

Attribute	Values	Description
DN length	3, 4, 5, 6, 7	The DN length setting allows you to change the number of digits for all DNs. The maximum length is seven. The default and minimum length is **3**.

3 Press <TAB> to save the new DN length.

The prompt appears: *If Business Communications Manager Voice Messaging is installed all messages and mailboxes will be deleted.*

4 Click **OK** to save the new DN length.

Note: Click **Cancel** to restore the original value.

5 On the navigation tree, click on Received # length.

The Received # length screen appears in the right frame.

6 Table 55 lists the possible values that can be entered for Received # length.

Table 55 Received # length values

Attribute	Values	Description
* Received # length	2, 3, 4, 5, 6, 7	The Received number length setting determines the number of digits the system reads to determine where to send the call. This setting allows you to change the number of digits received on auto-answer trunks. These digits identify target lines, Auto DNs, and DISA DNs.
	Tips: The target line number (for example, line 241) and the Received number for the target line (for example, Received number: 123 maps to line 241) must be different numbers. The Received number length can be the same as the system DN length, or may, because of network or central office constraints, be set to a lesser value. This number cannot be greater than the system DN length on a networked system using a coordinated dialing plan (CDP) or a universal dialing plan (UDP). On a stand-alone system it is possible that the received number length would be greater than the DN length **WARNING**: Changing the Received number length clears all programmed received digits.	

Direct Calling from Inside and Outside the System

This section dicusses setting up direct dialing from internal and remote sets, and setting up target lines.

Creating Direct Dial Sets

The Direct dial setting allows you to dial a single system-wide digit to call a specific telephone, called a direct dial telephone. The most common example of a direct dial set is a telephone for an operator, a receptionist or an attendant. You can program a maximum of five direct dial sets on the system.

To configure Direct dial sets:

1. Click the keys beside **Services**, **Telephony Services**, **General Settings**, and **Direct dial**.
2. Click the Set you want to program (**Set 1**-**Set 5**).

   The Set # window appears.
3. Use Table 56 to determine the settings you want to define direct dial sets.

Table 56 Direct dial values

Attribute	Values	Description
Type	Internal, External, None	This is the type of number for the direct-dial set.
Internal/External#	DN <number>	The DN number of the set to be designated as the direct dial set. (Internal sets). The actual phone number of the direct dial set (External sets).
Facility	Pool A to 0, Use prime Line, Use routing table	If you assign an external number as a direct dial set, you must indicate what line to use for the call.

Tips: There is one direct-dial digit for the entire system.

The Business Communications Manager cannot verify that the number you assign as an external direct dial set is valid. Check the number before assigning it as a direct dial set by calling the direct dial you have assigned.

Direct Dial Matrix

To help you with your direct dial planning, transfer the following information to a spreadsheet and fill out the values for each target line you create.)

Table 57 Direct dial sets

Direct Dial Set			
Set 1 Set 2 Set 3 Set 4 Set 5	None	Internal #	External # Use Prime line Use line Pool code_____ Use routing table

Creating Target Lines

Target lines are virtual direct links the Business Communications Manager makes between internal sets and the external trunks. By assigning target lines, you program the system to target a specific set when it receives a specific incoming number sequence.

1 Ensure you have analog DID (Direct Inward Dialing) lines or T1 or PRI lines with DID emulation.

Note: You also require target lines to receive calls received over a VoIP trunk. Refer to the *IP Telephony Configuration Guide* for details.

2 Click the keys beside Services, Telephony Services, System DNs, Active Set DNs.

3 Choose the DN of the set where you want the line to be directed.

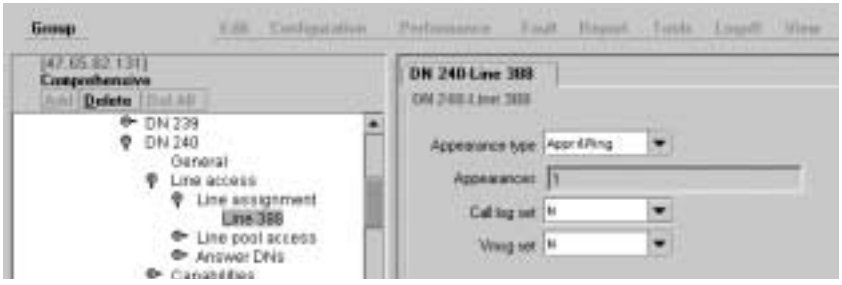
4 Choose Line assignment and click the Add button.

5 Enter the number of the target line you want to assign to the set (241-412).

6 Click on the line number. The DN/Line screen appears in the right frame.

7 Ensure that Appearance type is set to Appr & Ring. Refer to Figure 23.

Figure 23 Assigning a line to a set



8 Click the keys beside Services, Telephony Services, Lines, Target Lines, and the Line XXX you want to set.

9 Click the key beside Trunk/line data.

10 Click on Received number. Refer to Figure 24.

11 In the Private number field, enter the extension number assigned to the DN from step 3.

Figure 24 Defining a Received number

12 Press <Tab> to save the changes.

You can now receive calls dialed in to that extension.

Target Lines Matrix

To help you with your target line planning, transfer the following information to a spreadsheet and fill out the values for each target line you create.

Table 58 Target line record

Target line no. (3 digits)	Entered in target DN record with appearance and ring?
Telephone number (DN)	
Line type	Public Private to:_____
Rec'd #	None DN
Prime Set	221 None
CLID Set	None DN
Use Aux. ringer	Y N
If busy	PrimeSet BusyTone
Distinct Ring	None 2 3 4

Creating Direct Inward System Access (DISA)

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a COS password that determines what they are allowed to do in the system.

Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default. For DISA programming instructions, refer to Table 21 on page 112.

Tips: You cannot configure T1 DID trunks to answer with DISA. If you want incoming T1 DID calls to be answered with DISA, configure the system with a DISA DN. Incoming T1 DID calls that map onto the DISA DN are then routed to a line that has DISA.

Using Dialing Plan Settings

The dial plan you choose determines the type of numbering required to access a public and private network by defining the DN lengths for the codes that access the networks. You can define only one private network.

Dialing Timeout

Dialing timeout specifies how long the Business Communications Manager waits between user-dialed digits. This value allows Business Communications Manager to determine when the user stops dialing.

The user can also use the # key to indicate that they are finished dialing. This is not usually required except for international calls where the number of digits dialed varies.

To view or set the dialing time out, follow these steps:

1. Click the keys beside **Services**, **Telephony Services**, **General Settings**.
2. Click on **Dialing plan**.

   The Dialing plan window appears in the right frame.
3. In the **Dialing timeout** box select a timeout value (in seconds): **3, 4, 5, 6, 8, 10, 15**.

Note: A timeout value that is too small forces the caller to enter the digits very quickly. A timeout value that is too large causes the system to wait for extra time after the last digit is entered before the call is actually made.

For more information on non-PRI routing tables and destination codes, refer to “Routing Service” on page 256.

For more information on dialing rules in networking situations, refer to Chapter 9, “Configuring Public Networks,” on page 197.

Using Private Networking Dialing Plans

If your Business Communications Manager is part of a private network, you have a choice of dialing plans. However, all Business Communications Managers on a network must use the same type of dialing plan and have the same Private DN lengths to ensure proper call direction. Plan out these settings before you start programming for the network.

- UDP plans use a routing code and a location code plus the set DN (i.e. 6-403-XXXX) to determine where a call gets routed. You specify a Private DN length to allow all required digits to be dialed. Each node on the network has a unique three-digit location code.
- CDP plans use a unique steering code that gets dialed as part of the set DN (i.e. 2XXXX for one node, 3XXXX for another node, and so on) to determine where the call gets routed. Since each node on the network has a unique code, no other routing is required.
- The Meridian system administrator generates the Private Network IDs. These IDs are unique to each node on a network. Both UDP and CDP must include this code.

To set up a private network dialing plan, follow these steps:

1. Click the key beside **Services**, **Telephony Services**, **General Settings**, and **Dialing plan**.
2. Click on Private network.
3. Use Table 59 to determine which values to set so callers can access a private network.

Table 59 Private network values

Attribute	Values	Description
Type	None, CDP, UDP	You can specify if your Private network uses a coordinated dialing plan (CDP) or a universal dialing plan (UDP).
Location code	<unique three-digit number>	This code identifies this particular system for calls within the network for a UDP dialing plan. This number must be unique.
Private DN lengths	3-14	The Private DN lengths parameter specifies the length of DNs in the UDP dialing plan. This is used by all PRI calls where the route uses DN Type: Private. The system uses this number to determine how many digits need to be dialed to define the number as a private network call.
Private Network ID (CDP/UDP networks)	1-127	This is the unique number that identifies the system to the Meridian. This number is supplied by the Meridian system administrator.

Setting up Public Network Dialing

The Public network settings allows you to enter DN lengths for the networks the callers are allowed to dial, including special numbers such as 411 and 911.

The public DN lengths table is used for all PRI calls except those whose routes use service type Private or service type Tie with DN Type specified as Private. This table allows the Business Communications Manager to determine the length of a DN, based on the initial digits dialed.

A set of default Public DN lengths is included with the default template. In most cases it is not necessary to change the default values.

About the Public DN Lengths Table

In the public DN lengths table:

- You can define up to 30 entries.
- Each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 - 25).
- Several entries are predefined in North America. These defaults can handle most regions in North America without the need for additional programming. If required, you can remove or modify these entries.
- The table always contains one default entry.You cannot remove this entry.You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

Adding or modifying Public DN lengths

To add or modify Public DN lengths, follow these steps:

1. Click the keys beside **Services, Telephony Services, General Settings**, **Dialing Plan** and **Public network**.
2. Click on Public DN lengths.
3. At the top of the column, click Add.

   The Add Public DN Lengths dialog box appears.
4. In the DN prefix field, enter the prefix for the public network.
5. Click OK to exit the dialog box.
6. Repeat steps 4 and 5 until you have added all the public DNs you need.
7. On the menu, click the first Prefix number you added.

   The Prefix window appears in the right frame.
8. Enter the DN length for that prefix.
9. Press <TAB> to save.
10. Repeat for all DN length records you added or that you need to change.

Dialing Plans Matrix

To help you understand how you are using networking on your system, transfer the following information to a spreadsheet and fill out the information you chose.

Table 60 Dialing plan matrix

Private network	Type	Private Network ID	Location code	Private DN length
	None	N/A	N/A	N/A
	UDP			
	CDP			N/A

Public network	Pub DN length	DN prefix	DN length	

Configuring Remote Access

If you want callers from a different network or from the public network to be able to access your network lines, you need to set up remote access codes, and class of service (CoS) passwords to control outside access.

Remote Access Packages

The Remote access packages setting allows you to control the remote use of line pools.

Create a remote access package by defining the system line pools remote users can access. You then assign the package to individual lines, refer to “Use remote package” on page 96), and to a particular Class of Service password (see “COS Passwords” on page 184).

To define Remote access packages, follow these steps:

1. Click the keys beside **Services**, **Telephony Services**, **General settings**, and **Remote access packages**.
2. Click a Package number (**00** to **15**). The Package window appears.
3. Type in **Y** or **N** to enable remote paging for each pool in the Remote access package.

   Table 61 defines the variable found on the Package window.

Table 61 Private network values

Attribute	Values	Description
Remote page	Y, N	The Remote page setting allows you to determine if the Remote access package allows Remote paging.

4. Repeat steps 3 and 4 until you have defined all the package values you require.

Defining Line Pool Access for Remote Packages

Perform the following procedure for each package you defined in the previous section:

1. Click on the key beside **Line pool access**.
2. Click the **Add** button.

   The Add Pool Access dialog box appears.
3. In the Pool field, enter a line pool access code.
4. Click **Save**.
5. Repeat steps 1 to 4 for all packages you require line pool access codes for.

COS Passwords

Class of Service (COS) passwords permit controlled access to the system resources by both internal and remote users.

- When an internal user enters a COS password at a telephone, the restriction filters associated with the COS password apply instead of the normal restriction filters.
- Similarly, when a remote user enters a COS password on an incoming auto-answer line, the restriction filters and remote package associated with their COS password apply instead of the normal restriction filters and remote package.

The COS password can define the set of line pools that may be accessed and whether or not the user has access to the paging feature.

The COS that applies to an incoming remote access call is determined by:

- the filters that you apply to the incoming trunk
- the COS password that the caller used to gain access to Business Communications Manager.

In cases where DISA is not automatically applied to incoming calls, the remote caller can change the COS by dialing the DISA DN and entering a COS password.

Tips: Determine the Class of Service passwords for a system randomly and change them on a regular basis.
Users should memorize their COS passwords instead of writing them down. Delete employees' COS passwords when they leave the company. Typically, each user has a separate password. Alternately, several users can share a password or one user can have several passwords.
A system can have a maximum of 100 six-digit COS passwords (00 to 99). You can copy the restriction filters and remote package from one COS password to another. COS passwords must be unique.

Follow these steps to create COS groups and passwords:

1. Click the keys beside **Services**, **Telephony Services**, **General Settings**, and **COS Passwords**.

2 Click on a COS group (**COS 00-99**). The **COS** window appears in the right frame.

3 Use Table 62 to determine which values to set for each password.

Table 62 COS password values

Attribute	Values	Description
Password	6 digits	Enter a combination of numbers that the user needs to dial to get into the system.
User filter	None, Filter If you choose Filter, enter the two-digit user filter	User filter allows you to assign a restriction filter to a Class of Service password. The user filter associated with the Class of Service password replaces any normally applicable set restriction, line/set restriction, and remote restriction. The default setting (**None**), means that any normally applicable filters (set restriction, line/set restriction, or remote restriction) still apply.
Line filter	None, Filter If you select Filter, type in a two-digit line filter.	The **Line filter** box allows you to assign a specific line restriction to a Class of Service password. The line filter associated with the Class of Service password replaces any normally applicable line restriction. The default setting (**None**), means that any normally applicable line filter still applies.
Remote package	None, Package If you select Package, enter a two-digit remote package.	Refer "Remote Access Packages" on page 183 for more information.

Remote Access Matrix

To help you organize your external access, transfer the following information to a spreadsheet and fill out the external access information you want to use.

Table 63 Remote access matrix

Pswd # (00-99)	Assigned to (owner of password)	Password	User filter	Line filter	Remote pkg
			None Filter #	None Filter #	None Filter #
Remote access packages					
Package #	Line pool access A: **9** B: _____ C:_____ D:_____ E:_____ F:_____ G:_____ H:_____ I: _____ J: _____ K:_____ L:_____ M:_____ N:_____ O:_____ PRI-A: _____ PRI-B: _____				

Configuring Call by Call Limits

Call by Call service selection (CbC) allows you to access services or private facilities over a PRI line without the need for dedicated facilities. The different services represent different types of access to the network. Table 64 shows available services. Availability depends on the line protocol you choose.

Note: At least one module must be designated as PRI before the information under this heading appears.

Supporting protocols

The following protocols support Call by Call limits:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250 (MCI, Sprint, Generic)
- AT&T 4ESS custom

Call by call services

Business Communications Manager supports the Call by Call Services listed in Table 64.

Table 64 Call by Call Services available on the system

Service	Description
Public	Public calls connect Business Communications Manager and a Central Office (CO). Business Communications Manager supports both incoming (DID) and outgoing (DOD) calls. Dialed digits conform to the standard North American dialing plan (E.164 standard).
Foreign Exchange (FX)	Foreign exchange service connects a Business Communications Manager site to a remote central office (CO). This provides the equivalent of local service at the remote location.
Tie	Tie lines are private incoming and outgoing lines that connect Private Branch Exchanges (PBXs) such as Business Communications Manager.
OUTWATS	Outward Wide Area Telecommunications: This outgoing call service allows a Business Communications Manager user to call telephones in a specific geographical area referred to as a zone or band. Typically a flat monthly fee is charged for this service.
INWATS	Inward Wide Area Telecommunications: This long distance service allows a Business Communications Manager user to receive calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
International INWATS	An international long distance service that allows a Business Communications Manager user to receive international calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
Switched Digital	This service provides premises to premises voice and data transport with call management and monitoring features.

Table 64 Call by Call Services available on the system (Continued)

Service	Description
Nine Hundred	This service is commonly referred to as fixed charge dialing.
Private	Private incoming and outgoing calls connect Business Communications Manager to a virtual private network. Dialed digits can conform to the standard North American dialing plan (E.164 standard) or the dialed digits can use a private dialing plan.

Switches Supporting Call by Call Limits

Table 65 lists the service types and cross-references them with four common switches.

Table 65 Switches and service types chart

Service types[1]	NI-26	DMS-100 (custom)	DMS-250 (MCI, Sprint, Generic)	AT&T 4ESS
FX	FX	FX[2]	N/A	N/A
Tie[3]	Tie	Tie	Tie	SDN (software defined network)
INWATS	INWATS	INWATS	Eight Hundred	Toll Free MEGACOM
International INWATS	Same as INWATS	Same as INWATS	Same as INWATS	International Toll Free Service
OUTWATS	IntraLATA OUTWATS OUTWATS with bands InterLATA OUTWATS	OUTWATS	PRISM	MEGACOM
Private		DMS Private[5]	VNET (virtual network)	N/A
Switched Digital	N/A	N/A	N/A	ACCUNET[4]
Nine Hundred	N/A	N/A	Nine Hundred	MultiQuest
Public	Public	Public	Public	N/A

1. A shaded box indicates that the protocol does not support the service.
2. DMS-250 Sprint and UCS support incoming FX only (i.e. Network-to-Business Communications Manager). DMS-250 MCI does not support FX.
3. NI-2 allows two Tie operating modes: senderized and cut-through. Business Communications Manager supports only senderized mode.
4. Rates greater than 64 kbps are not supported.
5. Bell Canada VNET.
6. Not all service types may be supported by a switch type. For information, contact your service provider.

Provisioning for Call by Call Limits with PRI

To program the system for Call by Call Limits with a PRI interface, you must:

- provision a DTM as PRI, if one is not already configured as part of the system
- select a protocol, on page 99
- program incoming call routing, on page 152
- program routes that use the PRI pools, see "Configuring Call Routing" on page 117.

Other Required Programming in the Unified Manager

Programming Call by Call on PRI requires these settings:

- under **Line Access**, assign the line pool
- under **Services**, in routing services, assign a pool for routing, and assign the service type and service id, if required
- under **General settings**, specify the minimum and maximum values for the pools

Setting CbC Limits

PRI pool limits for Call by Call services allows you to configure limits for service types without interacting with the CO. This feature sets the minimum and maximum number of incoming and outgoing calls per service type for the PRI pool.

The number of active calls are tracked. Whenever a call is setting up, a check determines if the call is allowed. Calls are not allowed if they exceed the maximum value for that service type or if they use lines needed to maintain the minimum value of other service types.

Follow these steps to program CbC Limits

1. Click on the keys beside **Services**, **Telephony Services**, **General settings**, and **CbC limits**
2. Click on the key beside a pool type (PRI-A to PRI-F).
3. Select a service. For example, Public

   The services that display depend on the PRI protocol.
4. Table 66 lists the possible values to enter into the pool fields.

Table 66 DN length values

Attribute	Values	Description
Minimum incoming	Default: 2	**Note**: The total of the minimum values for incoming or outgoing PRI services cannot exceed the total number of lines in the PRI pool. The maximum value for an incoming or outgoing PRI service cannot exceed the total number of lines in the PRI pool.
Maximum incoming	Default: 23	
Minimum outgoing	Default: 4	
Maximum outgoing	Default: 23	

PRI Line Pools

All lines in a PRI interface are in the same PRI line pool. This pool cannot contain any non-PRI lines. There is one PRI pool available for each PRI interface. Depending on the order that the modules are configured as PRI, Pool PRI-A represents lines 061 to 083, Pool PRI-B represents lines 085 to 107, and Pool PRI-C represents lines 109 to 131, etc. to Pool PRI-F. If all PRIs are connected to the same service provider and use the same protocol, lines 061 to 083, 085 to 107, and 109 to 1311 etc. can be put in the same pool, PRI-A, PRI-B, PRI-C up to PRI-F.

CbC Matrix

To help you organize your PRI call by call limits lines, transfer the following information to a spread sheet and fill out the information.

Table 67 CbC matrix

PRI pool	**Type**	Incoming lines	Outgoing lines
PRI-A **PRI-B**	**Public Tie** **Foreign Exchange** **OUTWATS INWATS** **International INWATS** **Switched Digital** **Nine hundred** **Private**	Minimum incoming: _____ Maximum incoming: _____	Minimum outgoing: _____ Maximum outgoing: _____

Defining Restriction Filters

Restriction filters allow you to restrict the numbers that can be dialed on any external line within Business Communications Manager. Up to 100 restriction filters can be created for the system.

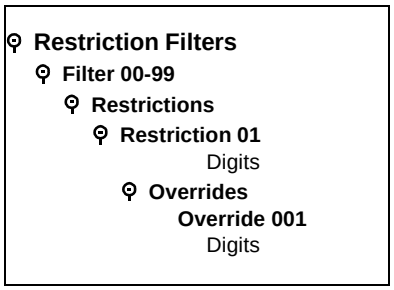
To restrict dialing within the system, you can apply restriction filters to:

- outgoing external lines (as line restrictions)
- telephones (as set restrictions)
- external lines on specific telephones (as line/set restrictions)

Restriction filters can also be specified in Restrictions service for times when the system is operating according to a schedule. Dialed digits must pass both the line restrictions and the set restrictions. The line per set (line/set) restriction overrides the line restriction and set restriction.

Figure 25 shows the Restriction Filters headings.

Figure 25 Restriction Filters headings



Notes About Restriction Filters

A restriction filter is a group of restrictions and overrides that specify the external numbers or feature codes that cannot be dialed from a telephone or on a line. The restriction filters setting allows you to assign restrictions in one step as a single package of dialing sequences that are not permitted.

In addition to restricting telephone numbers, you can prevent people from entering dialing sequences used by the central office (the public network) to deliver special services and features. Because some of these features provide the caller with dial tone after they have entered the special code (which often uses # or *), users have an opportunity to bypass restrictions. To prevent this from happening, you can create filters that block these special codes.

You create a filter by defining the dialing sequences that are denied. There are also variations of each sequence that you want users to be able to dial. Sequences that can be dialed are called overrides.

Once you create the filters, you can assign the restrictions to a telephone (**Terminals & sets**), to a line (**Lines**), to a particular line on a telephone (**Terminals & sets**), and to remote callers (**Lines, Remote access**).

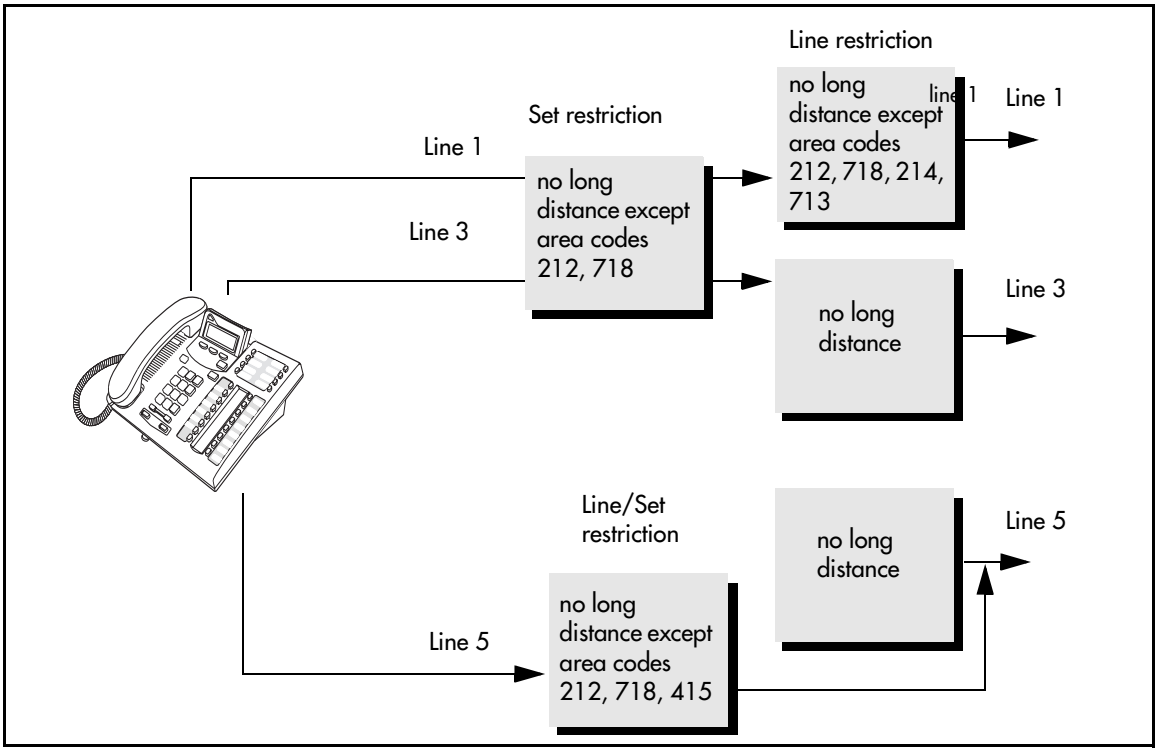
Note: Filter 00 cannot be changed. Filter 01 has a set of defaults. Filters 02 to 99 can be set to suit your special requirements.

See "Default Filters (North America)" on page 194.

- Each programmable filter can have up to 48 restrictions.
- There is no limit on the number of overrides that can be allocated to a restriction. However, there is a maximum total of 400 restrictions and overrides allocated to the 100 programmable filters.
- The maximum length of a restriction is 15 digits. The maximum length of an override is 16 digits.
- A single letter (A) in a dialing sequence is a wild card (stands for any digit).
- You can use * and # in a sequence of numbers in either a restriction or an override. These characters are often used as part of feature codes for other systems or for features provided by the central office (the public network).
- When restricting the dialing of a central office feature code, do not forget to create separate restrictions for the codes used for DTMF and pulse lines (for example, *67 and 1167).
- Do not string together a central office feature code and a dialing sequence that you want to restrict. Create a separate restriction for each.
- You can copy restrictions and overrides from one filter to another. You can use a restriction or override in any number of filters. Each time you use a restriction or override, it counts as one entry. For example, if restriction 411 exists in filters 01, 02 and 03, it uses up three entries of the 400 entries available.
- Removing a restriction from a filter has no effect on the contents of other filters even if the restriction was copied to them.
- You cannot delete a filter. Removing the restrictions programmed on a filter makes it an unrestricted filter but the filter itself is not removed.

Line and set restrictions are shown in Figure 26 and Figure 27 on page 192.

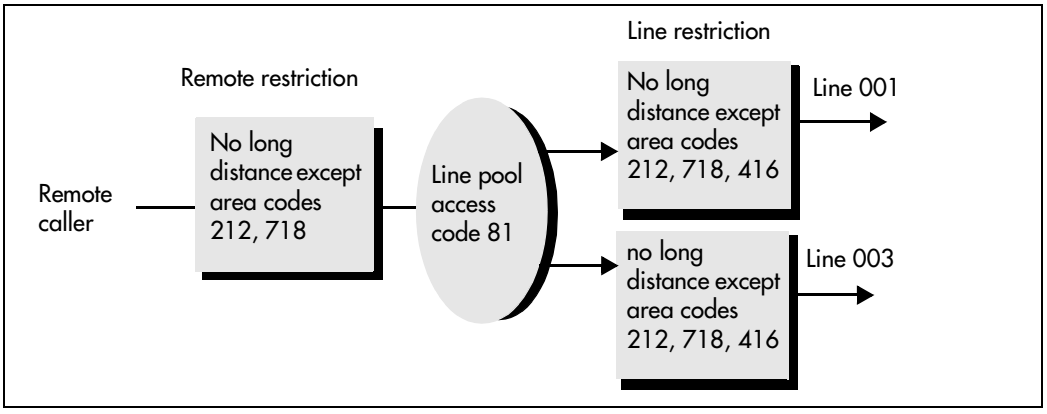
Figure 26 Line restriction example



In Figure 27, a caller using line 001 could only dial long-distance numbers to area codes 212 and 718. A caller using line 003 could not dial any long-distance numbers. A caller using line 005 could dial long-distance numbers to area codes 212, 718, and 415.

Tips: To restrict dialing from outside the system (once a caller gains remote access), apply restriction filters to incoming external lines (as remote restrictions).

Figure 27 Remote line restriction example


Line restriction
Remote restriction
Remote caller
No long distance except area codes 212, 718
Line pool access code 81
No long distance except area codes 212, 718, 416
no long distance except area codes 212, 718, 416
Line 001
Line 003

In this case, dialed digits must pass both the remote restriction and the line restriction. A remote caller can override these filters by dialing the DISA DN and entering a COS password.

Programming a Restriction Filter

Follow these steps to set up restriction filters:

1 Click on the keys beside **Services**, **Telephony Services**, **Restriction filters**, and the Filter you want to program (Filter 00-99).

2 Add or modify a restriction number:

a If you want to add or modify restrictions, click on **Restrictions**, then click the Add button at the top of the column.

b In the Digits field, enter the number or symbol you want to be restricted.

A new Restriction # listing is created.

c Click the Save button.

Warning: To remove restrictions that no longer apply, click on the Restriction # you want to remove, then click the Delete button at the top of the column.

Exercise caution when removing overrides.
If you remove a restriction, the overrides associated with the restriction are also removed. This action also changes the identifying numbers of the subsequent restrictions that you have defined. For example, if you remove Restriction 01, Restrictions 02 to 08 are renumbered as 01 to 07.

---

3 Click the key beside the Restriction number you created, to show the overrides listings.

4 Click the key beside **Overrides.**

If there are overrides for the restriction, a list of overrides appears.

5 Add or modify overrides:

a Click Overrides, and then click the Add button at the top of the column.
The Add Overrides dialog box appears.

b In the Digits field, enter the number that you want to be able to override the restriction filter.

Note: Enter the letter **A** as a wild card character that represents any digit in a sequence of numbers when denying numbers or creating overrides.

If you delete a restriction, it also deletes the overrides and the restrictions renumber to fill the gap.

---

c Repeat steps a and b for all the overrides you want to add

d Click the Save button.

Note: To delete an override: Select the override you want to delete, and then click on the Delete button at the top of the column.

If you want to delete all overrides for that restriction, click the Delete All button.

---

6 To view overrides, click on the override number you want to view.

Default Filters (North America)

Filter 00 permits unrestricted dialing and cannot be changed.

Filter 01 is pre-programmed with 10 restrictions and some associated overrides. In Filter 01, Restriction 02 and Override 001 allow long distance toll free calls.

The dialing string 911, which is the number for emergency assistance in North America, is included as both a restriction and an override in Filter 01. This arrangement prevents anyone from blocking calls for emergency assistance on lines or sets using the default filter.

Table 68 Default restriction filters

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	001: 1800 002: 1877 003: 1888
	03: 911	001: 911
	04: 411	
	05: 976	
	06: 1976	
	07: 1AAA976	
	08: 1900	
	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Note: Default filters are loaded only at a cold start.

Filters 02, 03, and 04, although not preset with restrictions and overrides, are the default filters in these programming headings:

Table 69 Default filters for program headings

Filter	Heading	Sub-heading
02	Terminals & sets	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

Restriction Filters Matrix

Transfer the following information to a spreadsheet and fill out the restriction filter information you want for your system.

Table 70 Restriction filters matrix

Filter #	Restriction #	Overrides			

Chapter 9
Configuring Public Networks

This chapter describes the ways of networking Business Communications Managers across a public network. Different countries have different trunk types, therefore these descriptions are also region based. Refer to "Trunk Availability by Region" on page 581 for more information.

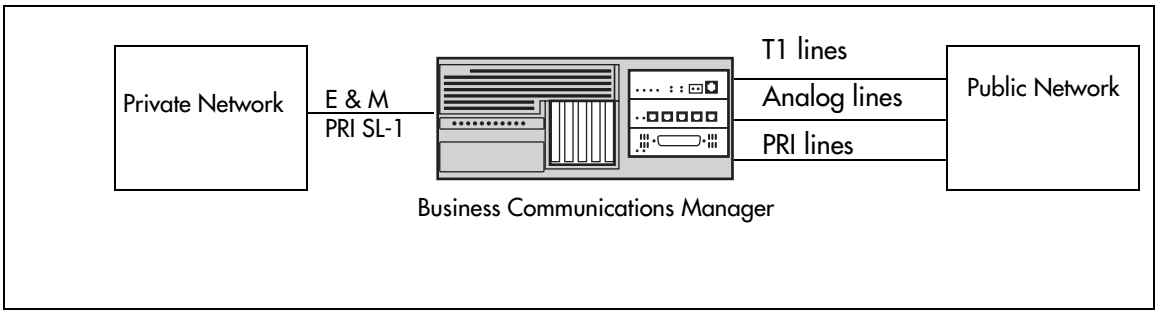
These are the protocols that the Business Communications Manager supports for public networking:

- PRI: ETSI Euro, NI, DMS100, DMS250, and 4ESS
- DASS2
- BRI: ETSI Euro, NI
- T1: Loop

Simple Networking

In the simplest form of networking, the Business Communications Manager acts as a routing station between a private network and the public network, as shown in Figure 28.

Figure 28 Connection to a private network



Call Access to the Business Communications Manager

In the above example, there are three types of callers:

- callers using the Business Communications Manager
- callers using the public network
- callers using the private network

Each type of caller has a specific method of accessing the other two systems.

Callers Using Business Communications Manager

These callers can:

- call directly to a specific telephone
- select an outgoing line to access a private network
- select an outgoing line to access features that are available on the private network
- select an outgoing central office line to access the public network
- use all of the Business Communications Manager features

Callers in the Public Network

These callers use the public lines to:

- call directly to one or more Business Communications Manager telephones
- call into Business Communications Manager and select an outgoing tie line to access a private network
- call into Business Communications Manager and select an outgoing central office line to access the public network
- call into Business Communications Manager and use remote features

Callers in the Private Network

These callers use private lines to:

- call directly to one or more Business Communications Manager telephones
- call into Business Communications Manager and select an outgoing tie line to access other nodes in a private network
- call into Business Communications Manager and select an outgoing central office line to access the public network
- call into Business Communications Manager and use remote features

Dialing Plans for T1 Lines

Business Communications Manager has a routing feature that allows you to set up a coordinated dialing plan with other systems in the public network. The goal is to have a network-wide dialing plan where all telephone numbers are unique and of a uniform length.

Typically, you use coordinated dialing plans with a network of systems with a three to seven digit dialing access between them.

Any programming for routing must be carefully planned using tables. For more information about routing and destination codes, see “Configuring Call Routing” on page 117. This section deals with applying the programming in network situations.

Dialing Plan Using Public Lines

The following illustrations provide an example of how you can record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax and Vancouver. Without routing, a Business Communications Manager user in Toronto would have to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number, the user simply dials 3027. The same feature is available for Vancouver (604).

In the column Dial out, P stands for pause, a host system signaling option. Press [ ] 7 8 to insert a 1.5 second pause in the dialing string.

Figure 29 Routing service record: use pool

Routing Services (Services: Routing Service)		
Route # (000-999)	Dialout (if required) (max. 24 digits or characters)	Use Pool
100	1-2-902-585	(A) B C
101	1-2-902-585	(A) B C
102	1-2-604-645	(A) B C
103	1-2-604-645	(A) B C

Create unique route number

Specify dial out digits

Route through Pool A

Figure 30 Routing service record: Destination code

Routing service (continued)								
Dest code (Services: Routing Services: Dest Codes								
Service Schedule	Normal		Sched 1		Sched 2		Sched 3	
Sched name (max. 7 char.)	Normal		Night		Evening		Lunch	
DestCode (max. 7 digits)	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length
30	100	0	000	All	000	All	000	All
31	101	0	000	All	000	All	000	All
32	102	0	000	All	000	All	000	All
33	103	0	000	All	000	All	000	All

Create unique code

Specify which route to use

Use entire dial out string

Destination Code Numbering in a Network

Because the system checks the initial digits of a call against the routing tables, each type of internal or external call must begin with a unique pattern of digits. The following table gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Table 71 Destination code leading digits

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
8	Call Park Prefix
9	All PSTN Calls

In the table, 4 is used as the initial digit for the coordinated dialing plan, but 5, or 6 can also be used for this purpose.

Tips: When programming a button to dial a Network number automatically (autodial), network calls must be programmed as external autodial numbers, even though they resemble internal extension numbers.
Routes generally define the path between the Business Communications Manager system and another switch in the network, not other individual telephones on that switch.

Chapter 10
Configuring Private Networks

This chapter describes how to network Business Communications Managers together in a private tandem network, as well as how to integrate the Business Communications Manager into an existing private network. Different countries have different trunk types, therefore these descriptions are also region based. Refer to "Trunk Availability by Region" on page 581 for more information.

Private Networking Protocols

These are the protocols that the Business Communications Manager supports for private networking:

- PRI: ETSI QSIG, MCDN
- DPNSS
- BRI: ETSI QSIG
- T1: E&M
- VoIP trunks (Refer to the *IP Telephony Configuration Guide* for details)

Business Communications Manager systems can be networked together using Tie lines or E&M connections. Larger networks, or networks that are geographically spread out, can be chained together through faster PRI SL-1 connections or with voice over IP (VoIP) trunk lines. If a Meridian 1 is part of the SL-1 network, the network also provides Meridian Customer Defined Networking (MCDN) features, including enhanced trunking features, end-to-end user identification, and centralized voice mail and auto attendant off the Meridian.

Keycode Requirements

Keycodes are required to activate the protocols that are used to create private networking. You must purchase and install these codes before you can create any of the networks described in this chapter. Consult with your Nortel Networks distributor to ensure you order the correct keycodes for the type of network you want to create.

Remote Access to the Network

Authorized users can access tie lines, central office lines, and Business Communications Manager features from outside the system. Remote users accessing a private network configured over a large geographical area, can potentially also place long-distance calls through the network and avoid toll charges.

Lines Used for Networking

External (trunk) lines provide the physical connection between Business Communications Manager and other systems in a private or public network.

The Business Communications Manager numbers lines from 061 to 240. Default numbering depends on the trunk module positioning within the Business Communications Manager. Refer to "Configuring Media Bay Modules" on page 74.

Note: VoIP trunks

Although a VoIP gateway does not require physical trunk lines, it is simpler to think of them in the same way as actual trunk lines. Therefore, in the Business Communications Manager, lines 001 to 060 are used forVoIP Gateway (IP telephony) functionality. Refer to the *IP Telephony Configuration Guide* for details about configuring VoIP trunks.

Business Communications Manager networking configurations that use PRI lines, require specific modules, depending on the type of lines chosen.

- A DTM that is configured for PRI is used for incoming and outgoing calls (two-way DID). Incoming calls are routed directly to a Business Communications Manager telephone. Outgoing calls are made using the intercom key and dialing destination codes.
- A DTM configured for T1 has digital lines that are configured as Groundstart, E&M, Loop, or DID.

Target lines are virtual communication paths between trunks and telephones on the Business Communications Manager system. They are incoming lines only, and cannot be selected for outgoing calls. With target lines, you can concentrate incoming calls on fewer trunks. This type of concentration is an advantage of DID lines. Business Communications Manager target lines allow you to direct each DID number to one or more telephones. Target lines are numbered 241 to 336.

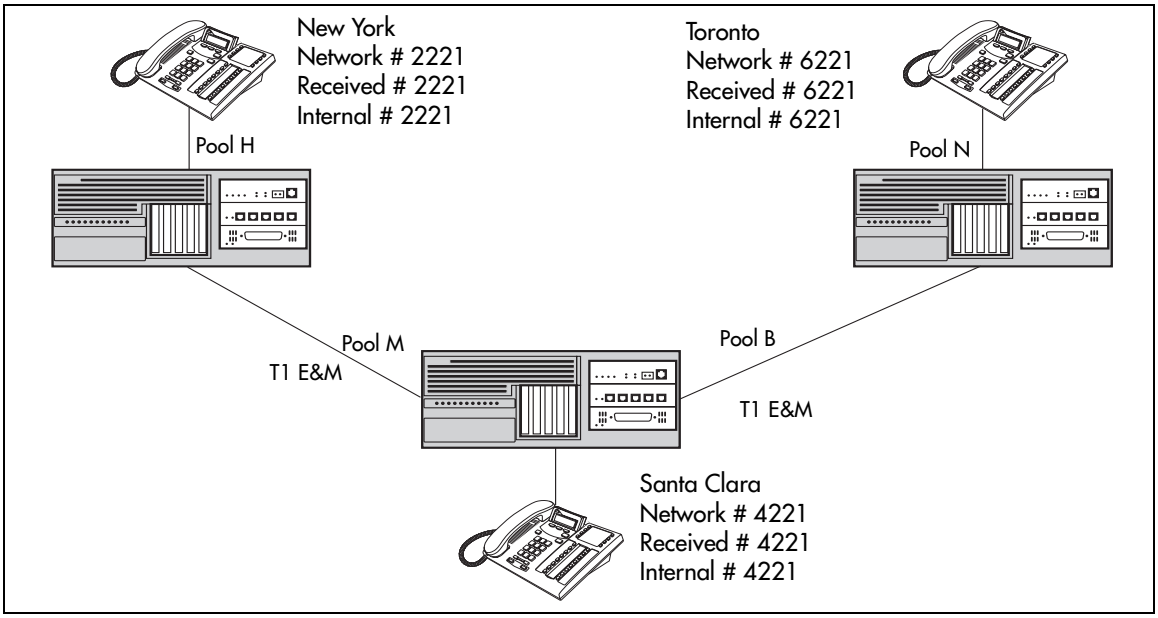
Telephones can be configured to have an appearance of any type of trunk and line (including target lines, excluding PRI trunks). If assigned, they are used for monitoring call usage.

Using Routing to Create Networking With T1 E&M Lines

By properly planning and programming routing tables and destination codes, an installer can create a numbering plan where T1 E&M lines between Business Communications Manager systems are available to other systems in the network

Figure 31 shows a network of three Business Communications Manager systems. Two remote systems connect to a central system.

Figure 31 Dialing plan for Business Communications Manager network



Each system must be running Business Communications Manager software. Each system must be equipped with target lines and Business Communications Manager with a DTM with at least one T1 E&M line or the appropriate Norstar trunk module configuration ported in through a Fiber Expansion module (FEM). Programming information for this network is shown in Table 72.

Table 72 E&M routing for a Business Communications Manager network

New York office:		
Heading	Parameter	Setting
Trunk/Line Data		
Network line (external)	Line 061	T1 E&M
	Answer Mode	Auto
	Line type	Pool H
Target line (internal)	Line 241	Target line
	Received #	2221
Line Access (set)	Set 2221	L241: Ring only
	Line pool access	Line pool H

Table 72 E&M routing for a Business Communications Manager network (Continued)

Heading	Parameter	Setting
Routing service	Route	001
	Use	Pool H
	External #	None
Routing Destinations	Office #1	Office #2
Routing to	Santa Clara	Toronto
Destination Code	4	6
Normal route	001	None
Absorb	None	001
Dialed number:	4221	6221
Santa Clara office:		
Heading	Parameter	Setting
Network line (external to NewYork)	Line 091	T1 E&M
	Answer Mode	Auto
	Line type	Pool M
Network line (external to Santa Clara)	Line 092	T1 E&M
	Answer Mode	Auto
	Line type	Pool B
Target line (internal to Toronto set)	Line 251	Target line
	Received #	4221
Line Access	Set 4221	L251: Ring only
	Line pool access	Line pool B Line pool M
Routing Destinations	Office #1	Office #2
Routing to	New York	Toronto
Route	001	002
Use	Pool M	Pool B
External #	None	None
Destination Code	2	6
Absorb	None	None
Normal route	001	002

Table 72 E&M routing for a Business Communications Manager network (Continued)

Heading	Parameter	Setting
Remote access	Rem access pkgs	01
	Line pool access	Pool M: ON
	Rem access pkgs	02
	Line pool access	Pool B: ON
	Line abilities	049
	Remote pkg	01
	Line abilities	050
	Remote pkg	02
Toronto office:		
Trunk/Line Data (external)		
	Line 093	T1 E&M
	Answer Mode	Auto
	Line type	Pool N
Target line (internal)	Line 300	Target line
	Received #	6221
Line Access	Set 6221	L300: Ring only
	Line pool access	Line pool N
Routing Destinations	Office #1	Office #2
Routing to	New York	Santa Clara
Route	001	
Use	Pool N	
External #	None	
Destination Code	4	2
Absorb	None	None
Normal route	001	001

If a user in New York wants to call Toronto within the network, they dial 6221. The local Business Communications Manager checks the number against the routing tables and routes the call according to the destination code 6, which places the call using Route 001.

The call appears on the auto answer line on the Business Communications Manager in Santa Clara as 6-221. Because 6 is programmed as a destination code for Toronto on the Santa Clara system, another call is placed using route 002 from Santa Clara to Toronto. At the Toronto system, the digits 6-221 are interpreted as a target line received number. The call now alerts at telephone 6221 in Toronto.

Tips: Network calls that use routes are subject to any restriction filters in effect.
If the telephone used to make a network call has an appearance of a line used by the route, the call will move from the Intercom button to the Line button.
The telephone used to make a network call must have access to the line pool used by the route.
Network calls are external calls, even though they are dialed as if they were internal calls. Only the features and capabilities available to external calls can be used.
When programming a button to dial a Network number automatically (autodial), network calls must be treated as external numbers, even though they resemble internal set numbers.
Routes generally define the path between your Business Communications Manager switch and another switch in your network, not other individual telephones on that switch.

Using Shared Line Pools to Create a Network

Using routes and destination codes is a powerful and efficient way to create a coordinated dialing plan. If the Business Communications Manager systems are close to each other geographically, you can conserve resources by not duplicating access. For example, system A, B, and C are all within the same area code. System A has a line pool to Santa Clara, System B has a line pool to Montreal, and system C has a line pool to Miami. An Business Communications Manager user in system A can reach Miami by calling system C and using their line pool to Miami.

To simplify access between Business Communications Manager systems, all line pools that go to the same destination should have the same line pool access code. For example, system A and system B both have a line pool to Ottawa.You can configure both systems with the same line pool access code for the Ottawa line pool.

A dialing plan similar to the one in Figure 32 on page 207 will let you create a company directory that uses line pool access codes and unique DNs of a uniform length

In this example, the person on system A at telephone 234 can press an Intercom button and dial 7434.

This means that telephone 234 has dialed the line pool access code of the trunk to system C, and will receive the dial tone of system C. The digits 434 then map to the Received number 434, and ring telephone 434 with an appearance of the associated target line.

Figure 32 Network example using shared line pools

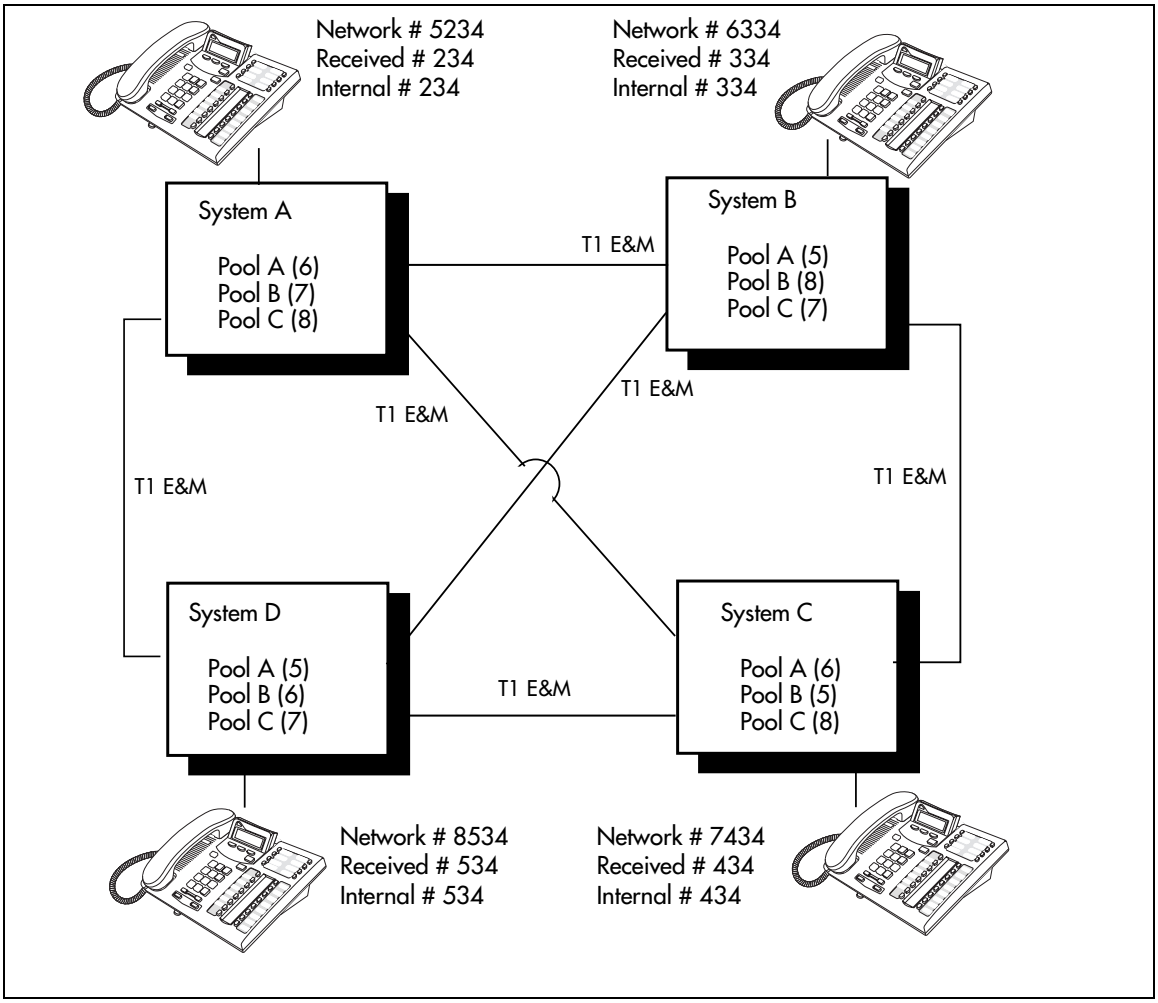


Table 73 shows the system coding for each system to set up a line pool-based coordinated dialing plan.

Table 73 Creating a coordinated dialing plan using line pools

Heading	Parameter	Setting		
Route from System A to:	System	B	C	D
Lines/Trunk/Line Data	Assign lines that connect with each system to a line pool	Pool A	Pool B	Pool C
General Setting/Access Codes/Line Pool Codes	Create an line pool access code for the pool	6	7	8
Dialout:		6334	7434	8534

Table 73 Creating a coordinated dialing plan using line pools

Heading	Parameter	Setting			
Route from System B to	System	A		C	D
Lines/Trunk/Line Data	Assign lines that connect with each system to a line pool	Pool A		Pool C	Pool B
General Setting/Access Codes/Line Pool Codes	Create an line pool access code for the pool	5		7	8
Dialout:		5234		7434	8534
Route from System C to	System	A	B		D
Lines/Trunk/Line Data	Assign lines that connect with each system to a line pool	Pool B	Pool A		Pool C
General Setting/Access Codes/Line Pool Codes	Create an line pool access code for the pool	5	6		8
Dialout		5234	6334		8534
Route from System D to	System	A	B	C	
Lines/Trunk/Line Data	Assign lines that connect with each system to a line pool	Pool A	Pool B	Pool C	
General Setting/Access Codes/Line Pool Codes	Create an line pool access code for the pool	5	6	7	
Dialout:		5234	6334	7434	

PRI networking using Call-by-Call Services

The example shown in Figure 33 on page 209 highlights the use of PRI Call-by-Call Services. It shows two offices of a company, one in New York and one in Toronto. Each office is equipped with a Business Communications Manager system and a PRI line. Each office has to handle incoming and outgoing calls to the public network. In addition, employees at each office often have to call colleagues in the other office.

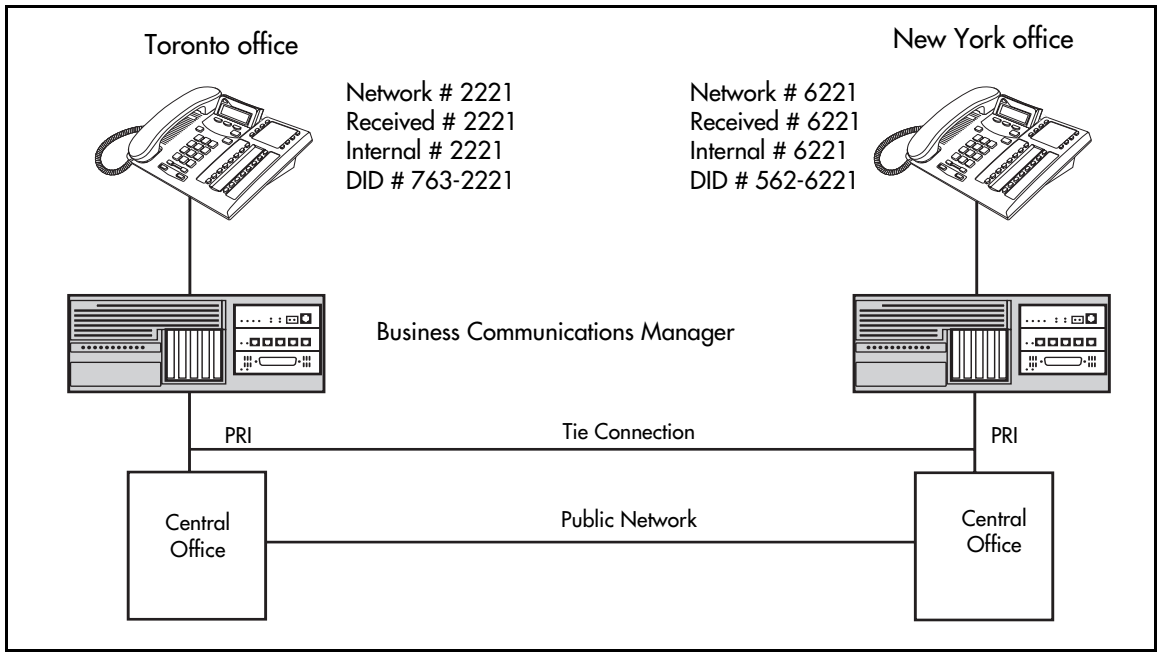
To reduce long distance costs, and to allow for a coordinated dialing plan between the offices, private lines are used to handle inter-office traffic. Refer to “Using Dialing Plan Settings” on page 180.

If call-by-call services were *not* used, each Business Communications Manager system might have to be equipped with the following trunks:

- 12 T1 DID lines needed to handle peak incoming call traffic.
- eight T1 E&M lines needed to handle inter-office calls.
- eight lines needed to handle outgoing public calls

The total required is thus 28 lines. If the Business Communications Manager systems were using T1 trunks, then two T1 spans would be required at each office. Note that the total of 28 lines represents the worst case value for line usage. In reality, the total number of lines in use at any one time will generally be less than 28. For example, during periods of peak incoming call traffic, the demand for outgoing lines will be low.

Figure 33 PRI networking using Call-by Call Services



With PRI Call-by-call services, it is not necessary to configure a fixed allocation of trunks. Each of the 23 lines on the PRI can be used for DID, private Tie, or outgoing public calls. This consolidation means that it may be possible for each office to use a single PRI span, rather than two T1 spans. With PRI Call-by-call services, the only limitation is that there are no more than 23 calls in progress at any one time.

The dialing plan at each Business Communications Manager site is configured to determine the call type based on the digits dialed by the user. If a user in Toronto wishes to dial a colleague in New York, they dial the four-digit private DN (such as 6221). The dialing plan recognizes this as a private network DN, and routes the call using Tie service with a private numbering plan.

Incoming Tie calls are routed to sets based on the digits received by the network, which in this case will be the four-digit private DN.

If a user in either location wishes to dial an external number, they dial ‘9’, followed by the number (such as 9-555-1212). The dialing plan recognizes this as a public DN, and routes the call using Public service.

Incoming DID calls will be routed to sets based on the trailing portion of the digits received by the network. For example, if a public network user dials an employee in the Toronto office, the network will deliver digits 4167632221. Business Communications Manager will route the call using the last four digits, 2221.

Refer to Table 74 for a description of the settings required for this type of routing service.

Note: Private network routing information appears in gray. Public network information appears in white.

Table 74 PRI call-by-call services routing information

Heading	Parameter	Home System Settings
Hardware	DTM	PRI
	Protocol	NI-2
Trunk/Line Data	Line 245	Target line
	Received #	2221
Line Access	Set 2221	L245:Ring only
	Line pool access	Line pool PRI-A
Routing Services	Private Network	Public network
	New York:	**Public network**
Route	001	002
External #	No number	No number
Use	Pool PRI-A	Pool PRI-A
Service type	Tie	Public
ServiceID	1	N/A
DN type	Private	N/A
Destination Code	6	9
Normal route	001	002
Absorb	0	ALL
New York office:		
Heading	**Parameter**	**Home System Settings**
Hardware	DTM	PRI
	Protocol	NI-2
Trunk/Line Data	Line 245	Target line
	Received #	6221
Line Access	Set 6221	L245:Ring only
	Line pool access	Line pool PRI-A

Table 74 PRI call-by-call services routing information

Routing Services	Private Network	Public Network
	Toronto	Public Network
Route	001	002
External #	No number	No number
Use	Pool PRI-A	Pool PRI-A
ServiceType	Tie	Public
ServiceID	1	N/A
DN type	Private	N/A
Destination Code	2	9
Normal route	001	002
Absorb	0	ALL

Private networking with PRI SL-1

The following section describes two of the private networking possibilities using Business Communications Manager equipment and PRI SL-1 lines.

The type of network you require depends on the equipment you are networking to, and how you want to use the network.

- You can tie a set of Business Communications Manager systems together to create a tandem network. This type of network provides the additional advantage of providing private line access to local PSTNs for all the nodes on the network.
- You can tie one or more Business Communications Manager systems to a Meridian 1 system and use the Meridian voice mail or auto attendant system for centralized call management, as well as providing reduced toll calling across the private lines.

You require PRI and MCDN keycodes to create either of these networking configurations. Note, however, that to use the MCDN features, your network must include a Meridian system as a controlling system.

System Numbering Plans

Both these types of networks require similar setups for dialing plans and routing. Each node must have a way to route external calls to the adjacent node or nodes. To do this, all nodes must have the same Private DN lengths.

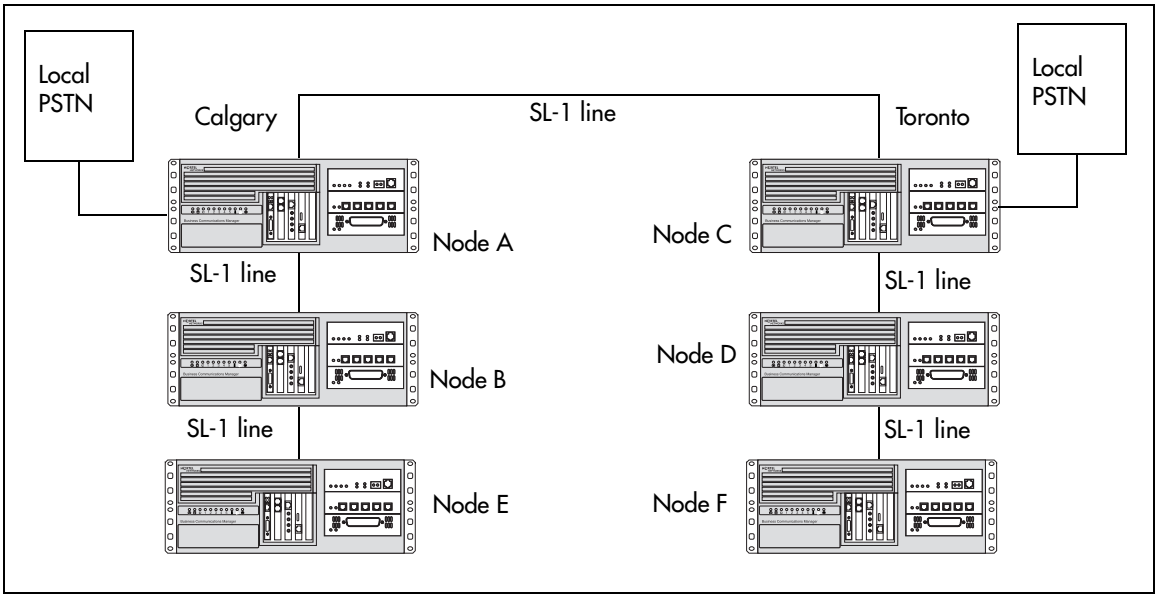
You use routing and a private dialing plan to control calls over the network. Refer to Chapter 8, “Controlling Access to the System,” on page 175 for a description of the two types of dialing plans available to private networks. Each example in this section describes the routing configurations that are required to support calls over the network.

Depending on the type of dialing plan you choose, each node must also have a unique location or steering code so the calls can be correctly routed through the nodes of the network. MCDN networks also require a Private Network ID, which is supplied by the Meridian network administrator to define how the Meridian system identifies each node.

Creating Tandem Private Networks

You can tie a number of Business Communications Manager systems together with SL-1 lines. This tandem network provides you with the benefits of end-to-end name display and toll-free calling over the SL-1 private link. Each Business Communications Manager becomes a node in the network.

Figure 34 Private tandem network between systems



In this type of network, you must ensure that each Business Communications Manager system, known as a node of the network, is set up to route calls internally as well as to other nodes on the system. This means, each node must have a route to the immediately-adjacent node, and the correct codes to distribute the called numbers. Each node must have a unique identification number, which is determined by the type of dialing plan chosen for the network.

As well, you can save costs by having a public network connection to only one or two nodes, and routing external calls from other nodes out through the local PSTN, thus avoiding toll charges for single calls.

Calls Originating from the Public Network

Table 75 Call originating from the public network to a tandem network

Received	Destination	Description
Node A	Node A	User in Calgary dials 761-xxxx number Incoming interface: Public DN type: Public
		Node A receives the call and identifies it as terminating locally. Uses target line to route call. Destination: Local (target line)
Node A	Node B	User in Calgary dials a 762-xxxx number DN type: Public
		Node A receives it and identifies it as being for node B. Uses private trunk to route it to B. Incoming interface: Public Destination: Remote Node Outgoing interface: Private
		Node B receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)
Node A	Node E	User in Calgary dials a 765-xxxx number. DN type: Public
		Node A receives it and identifies it as being for B. Uses private trunk to route call to B. Incoming interface: Public Destination: Remote node Outgoing interface: Private
		Node B receives it and identifies it as being for E. Uses private trunk to route call to E. Incoming interface: Private Destination: Remote node Outgoing interface: Private
		Node E receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)

Table 75 Call originating from the public network to a tandem network

Received	Destination	Description
Node A	Node C	User in Calgary dials a 761-xxxx number which is answered with DISA. Incoming interface: Public DN type: Public Destination: Local (DISA DN)
		User enters a COS password and a private DN for Node C i.e. 6 + 393-xxxx DN type: Private
		Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: (DISA user) Destination: Remote node
		Node C receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)
Node A	Node D	User in Calgary dials a 761-xxxx number which is answered with DISA. Incoming interface: Public DN type: Public Destination: Local (DISA DN)
		User enters a COS password and a private DN for Node D, i.e. 6 + 394-xxxx DN type: Private
		Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: (DISA user) Destination: Remote node
		Node C receives it and identifies it as being the responsibility of D. Uses private trunk to route call to D. Incoming interface: Private Destination: Remote node
		Node D receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)

Table 75 Call originating from the public network to a tandem network

Received	Destination	Description
Node A	Ottawa PSTN	User in Calgary dials a 761-xxxx number which is answered with DISA. User enters a COS password and an Ottawa public network number. Incoming interface: Public DN type: Public Destination: Local (DISA DN)
		Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: Local (DISA user) Destination: Remote PSTN
		Node C receives the call and identifies it as a public number and routes it out over the local PSTN. Incoming interface: Private Destination: Local PSTN

Calls Originating in the Private Network

Table 76 Calls originating from the private network within a tandem network

Received	Destination	Description
Node B	Node B	DN is internal, therefore no trunk routing is required. Incoming interface: Intercom DN type: Local Destination: Local
Node A	Ottawa PSTN	User in Node A dials the private network access code for Node C, followed by an Ottawa public number. Incoming interface: Intercom DN type: public Destination: Remote PSTN
		Node C receives the call and identifies it as being for the public network. Node C routes the call over the local public network. Incoming interface: Private DN type: Public Destination: Local PSTN
Node B	Calgary PSTN	User on Node B dials a public DN.
		Node B recognizes it as being the responsibility of Node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node
		Node A receives the call and identifies it as being for the public network. Node A routes the call over the local public network. Incoming interface: Private Destination: Remote PSTN

Table 76 Calls originating from the private network within a tandem network

Received	Destination	Description
Node B	Node A	User in Node B dials a private DN for a user on A. DN type: Private
		Node B recognizes it as being for Node A. Uses the private trunk to route the call the call to A. Incoming interface: Intercom Destination: Remote node
		Node B receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)
Node B	Node C	User on Node B dials a private DN for a user on C. DN type: Private
		Node B recognizes it as being the responsibility of Node A and routes the call over the private trunk to A. Incoming interface: Intercom Destination: Remote node
		Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Private Destination: Remote node
		Node C receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)
Node B	Node D	User on B dials a private DN for node D. DN type: Private
		Node B identifies it as being for node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node
		Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Private Destination: Remote node
		Node C receives it and identifies it as being for D. Uses the private trunk to route call to D. Incoming interface: Private Destination: Remote node
		Node D receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)

Table 76 Calls originating from the private network within a tandem network

Received	Destination	Description
Node B	Node F	User on B dials a private DN for node F. DN type: Private
		Node B identifies it as being for node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node
		Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Intercom Destination: Remote node
		Node C receives it and identifies it as being for D. Uses the private trunk to route call to D. Incoming interface: Intercom Destination: Remote node
		Node D receives it and identifies it as being for F. Uses the private trunk to route call to F. Incoming interface: Intercom Destination: Remote node
		Node F receives the call and identifies it as terminating locally. Uses target line to route call. Incoming interface: Private Destination: Local (target line)

Routing for Tandem Networks

In tandem networks each node needs to know how to route calls that do not terminate locally. To do this, you set up routes for each connecting node by defining destination codes for each route.

If the node is also connected to the public network, the usual routing is required for that connection.

Table 77 to Table 80 show the routing tables for Node A and Node C for external and internal terminating calls.

Note: The PRI lines are enbloc lines, so all dialed digits are collected before being dialed out.

Table 77 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4 (PSTN)	1	91604
3 (Node B)	0	91403762 (Node B)
3 (Node B)	0	91403765 (Node E)
4 (PSTN)	1	9140376* (not internal network)
4 (PSTN)	1	914037* (not internal network)

Table 77 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4 (PSTN)	1	91403* (not internal network)
4 (PSTN)	1	9* (not internal network)
* This wild card represents a single digit.		

Table 78 Node A destination code table, internal termination

Route	Absorb length	Destination code (private DNs)
3 (Node B)	0	392 (Node B)
3 (Node B)	0	395 (Node E)
5 (Node C)	0	393 (Node C)
5 (Node C)	0	394 (Node D)
5 (Node C)	0	396 (Node F)

Table 79 Node C destination code table, external termination

Route	Absorb length	Destination code (Public DNs)
3 (Node B)	0	91613764 (Node D)
3 (Node B)	0	91613766 (Node F)
4 (PSTN)	1	9161376* (not internal network)
4 (PSTN)	1	916137* (not internal network)
4 (PSTN)	1	91613* (not internal network)
4 (PSTN)	1	9161* (not internal network)
4 (PSTN)	1	916* (not internal network)
4 (PSTN)	1	91* (not internal network)
4 (PSTN)	1	9 (not internal network)

Table 80 Node C destination code table, internal termination

Route	Absorb length	Destination code (Private DNs)
3 (Node D)	0	394 (Node D)
3 (Node D)	0	396 (Node F)
5 (Node A)	0	391 (Node A)
5 (Node A)	0	392 (Node B)
5 (Node A)	0	395 (Node E)

Using SL-1 with MCDN to Network with a Meridian System

When you connect your Business Communications Manager systems through the SL-1 MCDN protocol to a Meridian 1, the Meridian system manages several aspects of the network, including voice mail, auto attendant services, and system timing.

Meridian System Requirements

When setting up networking with Meridian, the Meridian systems must provide the following:

- the correct software version to allow MCDN features (If your Meridian system administrator cannot confirm this, call your technical support center (TSC) or 1-800-4NORTEL.)

  The Meridian must provide the following:

  — end-to-end signaling (option 10)
  — message center (option 46) and an IVMS link (option 35)
  — Meridian Mail link (option 77 and 85)
  — basic Attendant Console Directory features (options 40, 45, and 83)
  — ISDN PRI or ISDN Signaling link (option 145 and 146 or 145 and 147)
  — advanced ISDN features (option 148)
  — network message services (option 175)
- act as the timing master for the private network connections
- use descending mode for PRI B-channel selection
- recognize dial codes for all nodes in the network.
- provide routing tables that direct incoming calls to the correct nodes on the network, including DID calls from the public network
- recognize the destination code (usually 9) that indicates a public network call, regardless of where in the network the number was dialed from.

Meridian MCDN Features

Table 81 lists the MCDN features that are provided by an SL-1 link to a Meridian system. The features affect messaging, trunking, and call attendant functions.

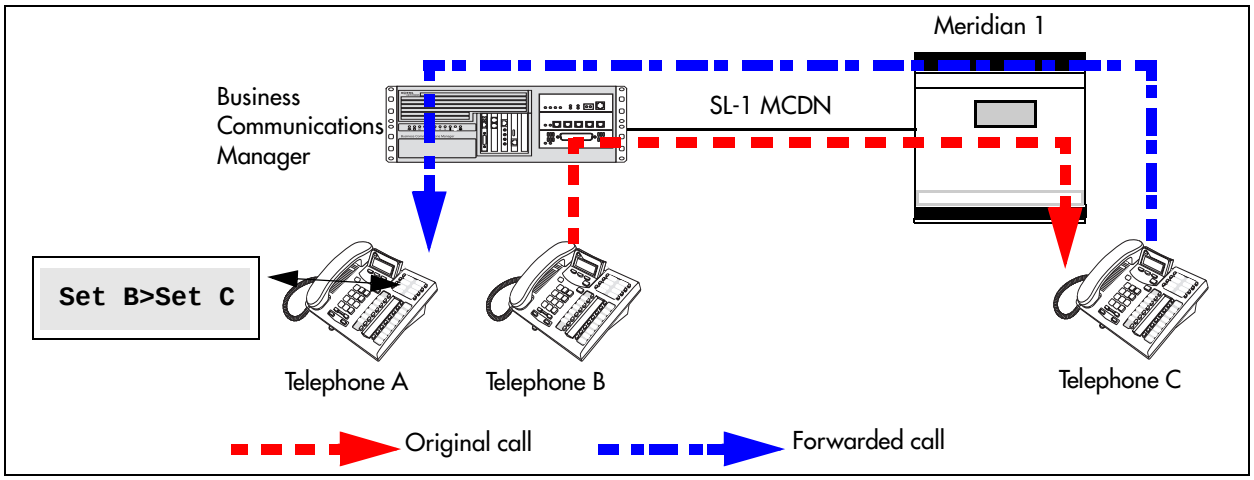
Table 81 MCDN feature enhancements

Centralized messaging	• network call transfer (NCT) • network call redirection information (NCRI) • message waiting indication (MWI)
Centralize trunking	• ISDN call connection limitation (ICCL) • trunk route optimization (TRO) • trunk anti-tromboning (TAT)
Centralized Attendant	• camp-on • break-in

Network Call Transfer

When a call is transferred over the MCDN network, both the destination telephone identifies the original name/number and the originating telephone receives the destination telephone information. Call identification is provided by the line. Figure 35 demonstrates this feature.

Figure 35 Network call transfer from a Meridian system



Network Call Redirection Information

NCRI builds on the following Business Communications Manager features:

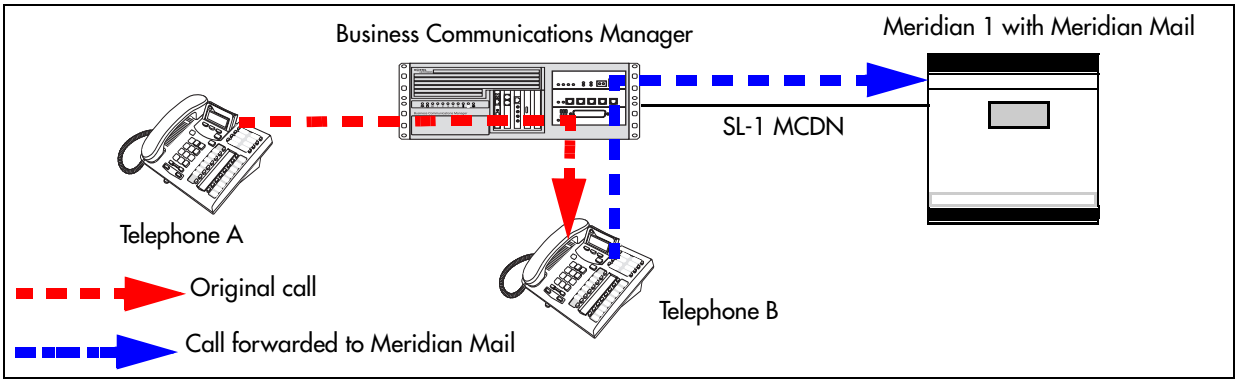
- External Call Forward
- Call Transfer
- Call Forward

NCRI adds the ability to redirect a call across an MCDN network using Call Forward (all calls, no answer, busy) and Call Transfer features. The call destination also receives the necessary redirection information. This feature allows the system to automatically redirect calls from within a Business Communications Manager system to the Meridian Mail system, which resides outside the Business Communications Manager system on the Meridian 1.

Figure 36 on page 221 shows an example of this situation, where user A calls user B on the same Business Communications Manager. If user B is busy or not answering, the call automatically gets transferred to a Meridian Mail number (user C) across an MCDN link between the Business Communications Manager system and the Meridian 1 system where the mailboxes are set up.

Refer to “Assigning Call Forward” on page 158.

Figure 36 Network call redirection path



Message Waiting Indication

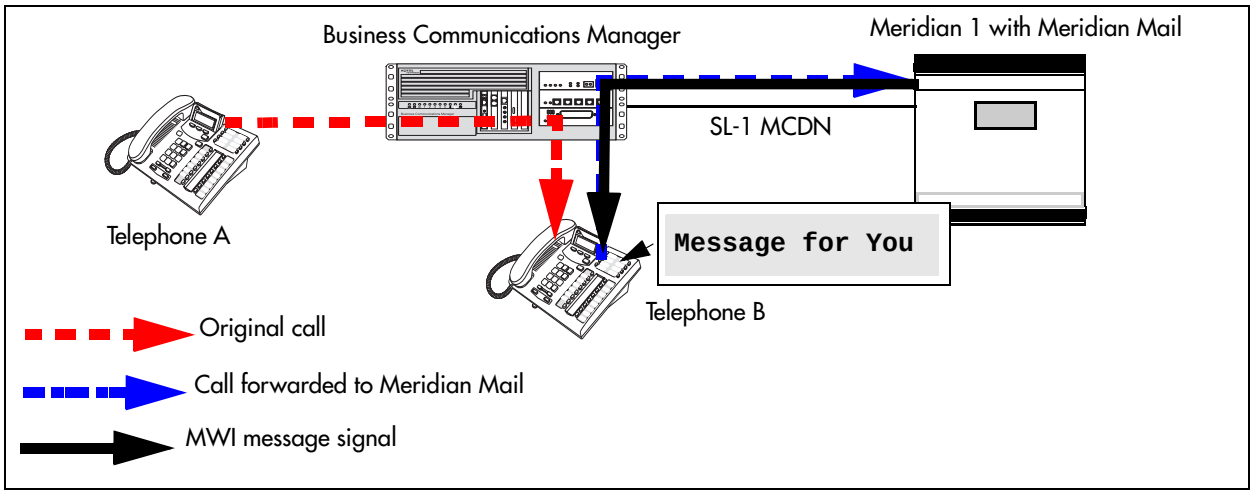
MWI allows the host system (Meridian 1) to notify a set on the Business Communications Manager of a call waiting.

Special requirements:

- Over a PRI SL-1 line: Meridian 1 must be on Release 19 or greater.
- Meridian 1 requires the network ID of the Business Communications Manager, which is defined under Dialing Plan/Private Network on the Business Communications Manager. This is a number between 1 and 27, and is defined by the Meridian system administrator.

Figure 37 demonstrates how the Meridian responds when a call is forwarded to a Meridian Mail mailbox.

Figure 37 Message waiting indication message



ISDN Call Connection Limitation

The ICCL feature piggybacks on the call initiation request and acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels.

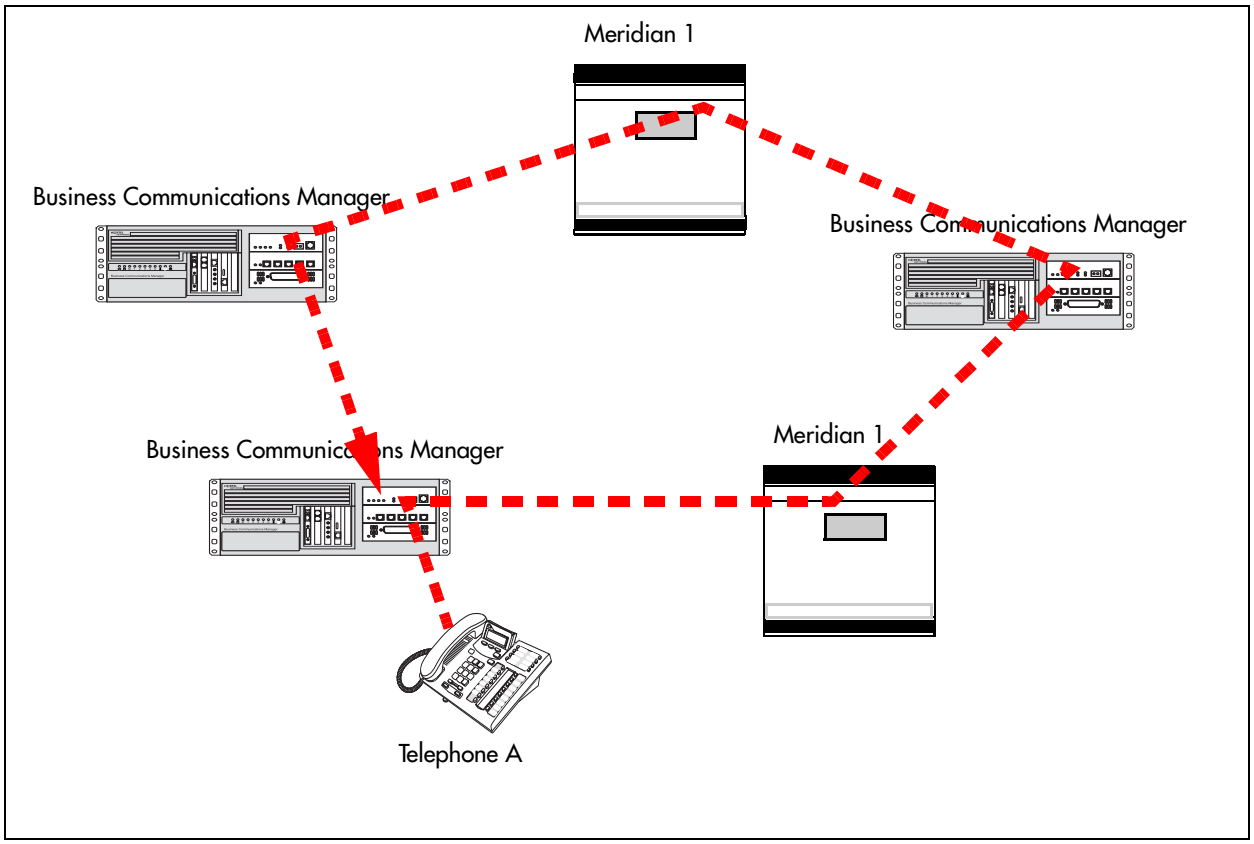
This feature adds a transit/tandem counter to a call setup message. This counter is compared at each transit PBX with a value programmed into the transit PBX, in a range from 0 to 31. If the call setup counter is higher than the PBX value, the call will be blocked at the PBX and cleared back to the network. This prevents calls from creating loops that tie up lines.

Business Communications Manager configurations:

- Under Network Settings/MCDN, set TRO to Y(yes).
- Under the media bay module record for the trunk module, define Maximum transits.

Figure 38 demonstrates how a call might loop through a network if the system is not set up with the ICCL feature.

Figure 38 Call loop on system without ICCL



Trunk Route Optimization

TRO finds the most direct route through the network to send a call between nodes. This function occurs during the initial alerting phase of a call.

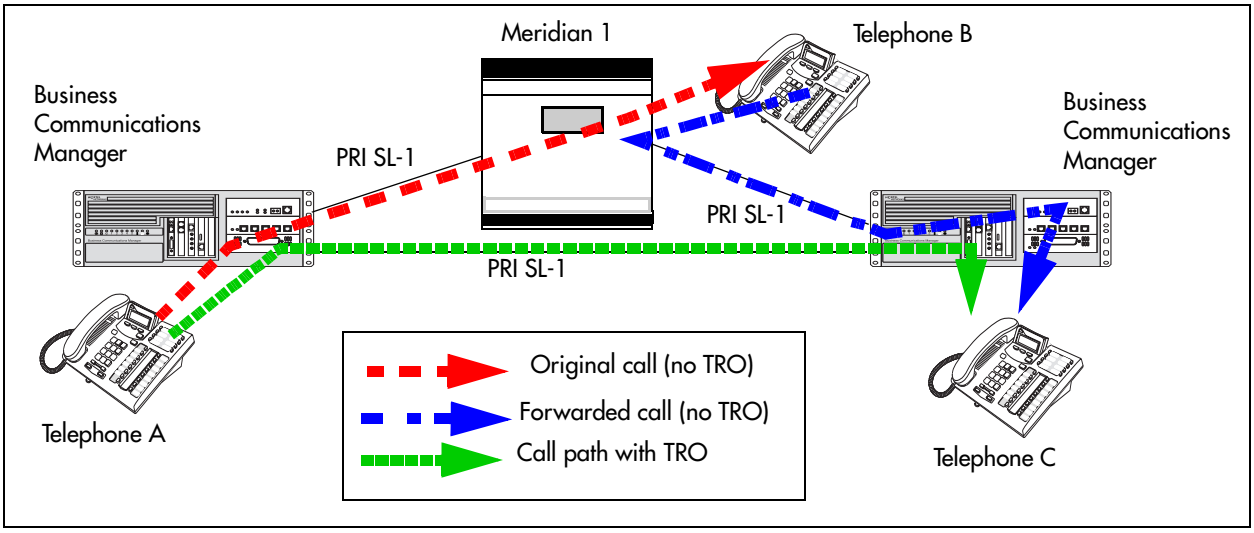
This feature avoids the following situation: A call originating from a Business Communications Manager system may be networked to a Meridian system, which, in turn, is networked to another Meridian system, which is the destination for the call. If the call routes through the first Meridian (M1) to reach the second Meridian (M2), two trunks are required for the call. A optimal choice is a straight connection to M2. This finds these connections and overrides the less-efficient setup.

Business Communications Manager configurations:

- Under Network Settings/MCDN, set TRO to Y(yes).
- Configure call routing for all optimal routes
- Configure **Call Forward** (All Calls, No Answer, Busy) or **Selective Line Redirection** to use the optimal routes.

Figure 39 shows two call paths. The first route, through the Meridian, demonstrates how a call might route if TRO is not active. The second route, that bypasses the Meridian, demonstrates how TRO selects the optimum routing for a call.

Figure 39 Call paths with and without TRO



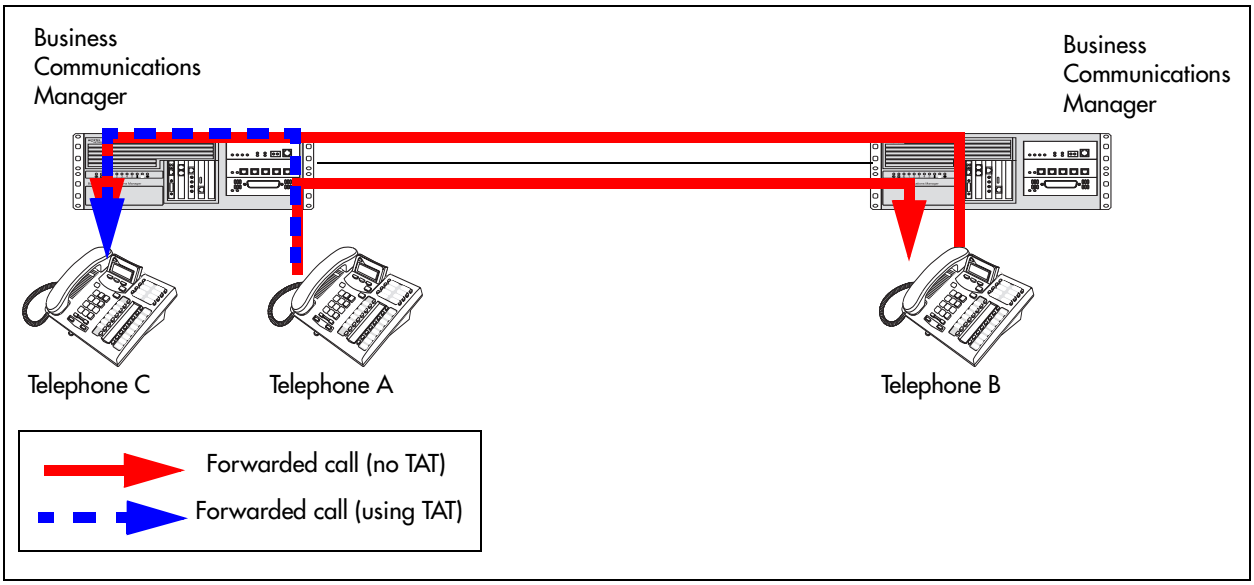
Trunk Anti-tromboning

TAT is a call-reroute feature that works to find better routes during a transfer of an active call. This feature acts to prevent unnecessary tandeming and tromboning of trunks.

Tips: This feature is not applicable for alerting calls.

Figure 40 shows how TAT reduces the line requirements. The solid line shows Telephone A calling Telephone B and being transferred over an additional PRI line to Telephone C. With TAT active, the same call is transferred to Telephone C over the same PRI line.

Figure 40 Call paths with and without TRO



Camp-on

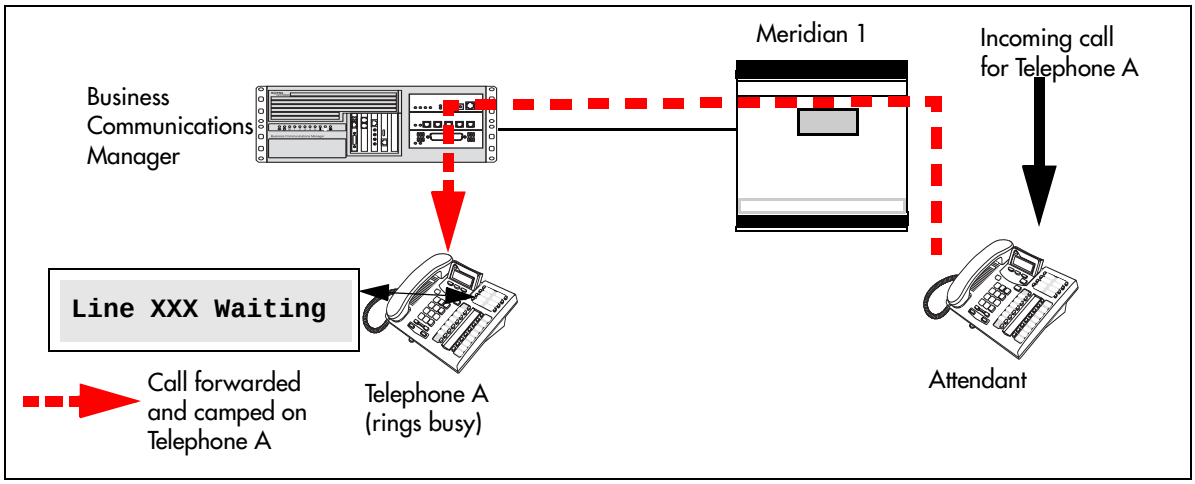
A call received by the Meridian attendant can be assigned to a telephone anywhere in the MCDN network, when the following situations are valid:

- the target telephone rings busy when the attendant calls
- no free keys on target telephone
- DND regular feature is inactive
- DND on busy feature is inactive

The target user sees that there is a call camped on the telephone. The called user can then clear a busy lines and take the call, or the user can choose to reject the call, using F814, or the user can indicate Do Not Disturb, using F85.

Figure 41 demonstrates the call path for a Meridian attendant to camp a call on a telephone in the Business Communications Manager system.

Figure 41 Camping a call



Break-in

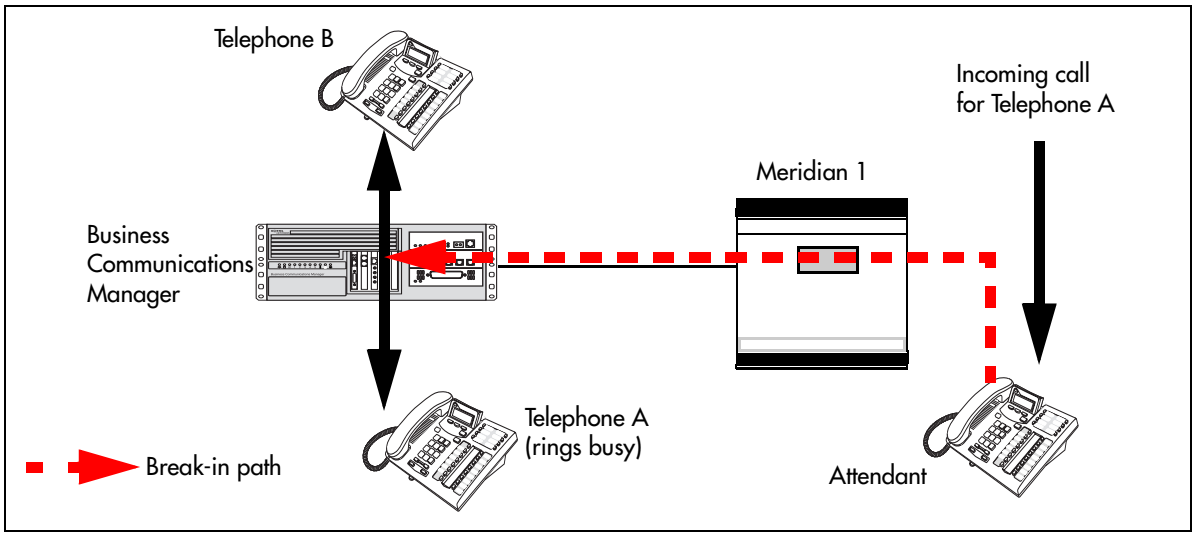
The Meridian attendant can break into an on-going call from a telephone in the Business Communications Manager system, if these situations are valid:

- Target Business Communications Manager telephone is busy but still has a free intercom or line key.
- DND busy is turned on, although the attendant can override a busy signal, if it is turned off, by pressing the **BKI** key.
- Prime set also should be busy, with no free key, and with DND turned on.
- Attendant capability is high (2), and higher than either the target telephone or the caller the target telephone owner is busy with.

A warning tone occurs for both parties on the call before the actual break-in occurs.

Figure 41 demonstrates the call path for a Meridian attendant to break into a call between telephones in the Business Communications Manager system.

Figure 42 Breaking into a Business Communications Manager call path



Break-in can be accomplished using two methods:

- Pre-dial BKI:
  1. Attendant presses BKI button on telephone.
  2. Attendant dials the destination number.
  3. On receiving a busy signal, the Attendant presses BKI again.

     Attendant is given access to the conversation.

- Post-dial BKI: Attendant:
  1. Attendant dials destination number.
  2. If a camp-on or busy tone is heard, the attendant presses the BKI button on the telephone.

     Attendant is given access to the conversation.

You can set a level of priority that will determine if a telephone will allow an attendant to break in. This is referred to as setting the Intrusion level. Use the following rules to configure the break-in feature.

- Set the Intrusion level for each telephone (under Capabilities). Refer to "Setting Intrusion Controls" on page 161.

  How the intrusion hierarchy works:

  — Break-in allowed if Attendant set is High and caller set is Medium.
  — Break-in is not allowed if Attendant set is Medium and caller set is high.

Creating an SL-1 Network

MCDN is supported over a PRI (LS-1) line trunk between your Business Communications Manager and a Meridian 1 system.

To set up a PRI connection on the Business Communications Manager side, you need to:

1. Ensure the Meridian 1 system is set up to accommodate your system on the network.
2. Install a DTM module which will be connected to the appropriate PRI trunk.
3. Enter the MCDN keycode.
4. Turn on the MCDN feature and set it to the proper line access.

   Services/Telephony Services/General Settings/Network Settings/MCDN
5. Put the lines assigned to the DTM module to the same line pool.
6. Ensure your dialing plan coordinates with what the Meridian and other nodes on the network are using **Services/Telephony Services/General Settings/Private Network/UDP or CDP.**
7. Enter the network system identifier the Meridian system administrator supplied (between 1 and 27).
8. Set up your numbering plan to recognize the network system identifiers of the other nodes on the system, so your system can pass them along, as required.
9. Set up routing to target the PRI line pool you set up and assign the pool to any telephones you want to allow to use this line.
10. Program target lines to match set extensions.
11. Set up the Meridian system voice mail DN as the voicemail DN for your system.
12. Test the link.

Figure 43 shows a private network composed of one central Meridian 1, and two sites with Business Communications Manager systems all connected by SL-1, with MCDN activated on all sites. This example uses a coordinated dialing plant (CDP). The DNs consist of four digits. The first digit is a destination code which is specific to each system, and contains the Location code, which uniquely identifies each system. The last three digits are unique to each telephone within that system. Refer to Chapter 8, “Controlling Access to the System,” on page 175 for a description of the dialing plans available to private networks.

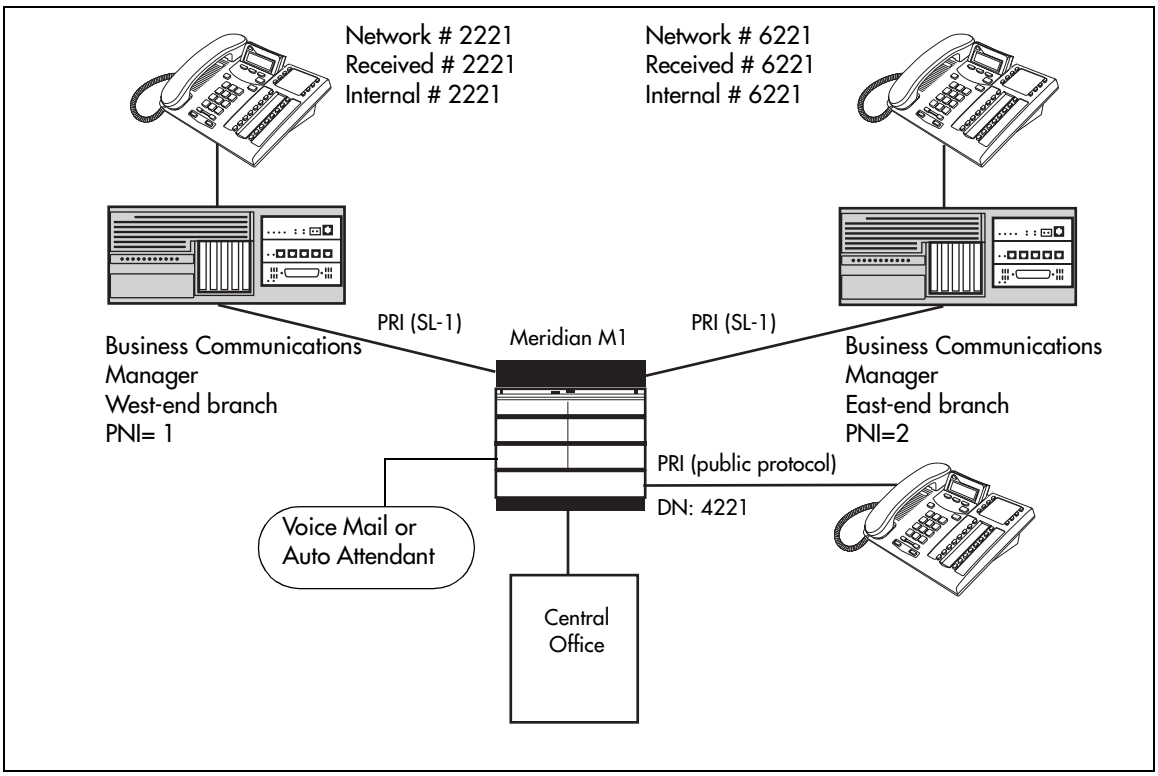
This example could represent a large head office (the Meridian 1) connected to several smaller branch offices (the two Business Communications Managers). In this network, only the head office has trunks connected to the public network.

The branch offices access the public network via the PRI to the head office. This configuration allows for cost savings by consolidating the public access trunks. Users at all three locations access the public network by dialing 9, followed by the public number. For example, a user in the West End branch might dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long distance call). These public calls are routed to the Meridian 1 by the Business Communications Manager routing table. Routing tables at the Meridian 1 will then select an appropriate public facility for the call.

Note that the Private Network Identifier (PNI) is programmed at each end of the links. The PNI identifies the Business Communications Manager to the Meridian 1 system.

Routing is set up such that network calls are made by dialing a four-digit private network DN. For example, if a user in the west end branch wishes to call a user in the east end branch within the private network, they dial 6221. Figure 43 illustrates this example.

Figure 43 MCDN networking, with a common public network connection



The implications on the configuration on each node to access the PSTN through one network node:

- Each node must have the Private Network Access Code set to the value 9.
- Each node must have destination code(s) that match the Private Network Access Code plus digits corresponding to calls terminating in the local PSTN. For example, if the Private Network Access Code is 9, the node in Ottawa would require a destination code of 91613. Similarly, Toronto would require the following destination code: 91416.

Business Communications Manager Module Settings

Table 82 lists the module settings that are required to set up the network described in Figure 43 on page 228. Refer to "Configuring Resources — Media Bay Modules" on page 71.

Table 82 Module settings for MCDN network

Heading	Parameter	Setting
West End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary
East End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary

Business Communications Manager Dialing Plan Settings

The following table lists the dialing plan settings that are required to set up the network described in Figure 43 on page 228. Also refer to "Using Dialing Plan Settings" on page 180.

Table 83 MCDN dialing plan settings

Heading	Parameter	Setting
West End office:		
Dialing Plan programming	Type	UDP
	Private Network ID	1
	Location Code	<unique three digits> (becomes part of destination code)
	Private DN Length	4
East End office:		
Dialing Plan programming	Type	UDP
	Private Network ID	2
	Location Code	<unique three digits> (becomes part of destination code)
	Private DN Length	4

Business Communications Manager Routing Information

Table 84 lists the lines and routing information required to set up the network shown in Figure 43 on page 228.

Note: In this example, the private DN length is 4. The public dialed DN length is 7.

Table 84 Network routing information

Heading	Parameter	Setting	
West End office:			
Trunk/Line Data	Line 245	Target line	
	Received #	2221	
Line Access	Set 2221	L245:Ring only	
	Line pool access	Line pool PRI-A	
Routing Services	Private Network		Public Network
	Head Office and East end		
Route	001		002
External #	No number		No number
Use	Pool PRI-A		Pool PRI-A
DN type	Private		Public
Destination codes for routes to:	Head office to M1	Head office to East End	
Destination Code	4(includes location code)	6	9
Normal route	001	001	002
Absorb	0	0	0
East End office:			
Trunk/Line Data	Line 245	Target line	
	Received #	6221	
Line Access	Set 6221	L245:Ring only	
	Line pool access	Line pool PRI-A	
Routing Services	Private Network		Public Network
	Head Office to West End		
Route	001		002
Dial out #	No number		No number
Use	Pool PRI-A		Pool PRI-A

Table 84 Network routing information (Continued)

DN type	Private		Public
	Head Office to M1	Head Office to West End	Call terminates at M1
Destination Code	4 (contains location code)	2	9
Normal route	001	001	002
Absorb	0	0	0

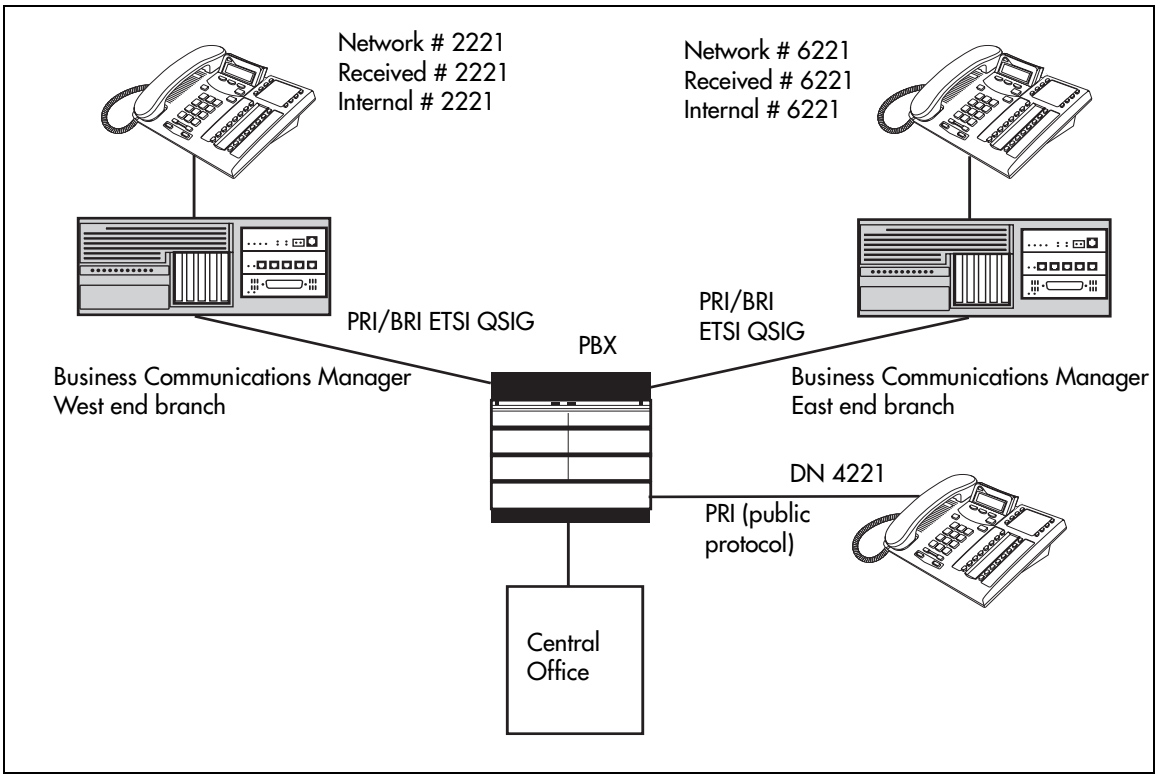
Networking with ETSI QSIG

(International systems only)

ETSI QSIG is the European standard signaling protocol for multi-vendor peer-to-peer communications between PBXs and/or central offices.

Figure 44 illustrates this example. Note that this is exactly the same setup as shown in Figure 43 on page 228, which describes PRI SL-1 networking. The exception in the configuration is for the hardware configuration because the trunk lines are different. The hardware programming for ETSI QSIG is described in "Hardware programming for the branch offices" on page 232. All other configurations are the same as those shown in Table 84 on page 230.

Figure 44 ETSI QSIG networking



Hardware programming for the branch offices

Table 85 lists the settings for some of the hardware parameters for ETSI QSIG networking example shown in Figure 44 on page 231.

Table 85 Hardware programming for branch offices

West End office:		
Heading	**Parameter**	**Setting**
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary
East End office:		
Heading	**Parameter**	**Setting**
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

ETSI Network Services

If your system has ETSI ISDN BRI/PRI lines, you can activate the malicious call identification (MCID) and Network Diversion features. Advice of charge-end call (AOCE) is active if your service provider has activated that service on the line.

When the features are activated, users can:

- display a call charge
- redirect calls over the ETSI ISDN BRI/PRI line to the outside network
- tag malicious calls

Advice of Charge-End of Call (AOCE) — AOCE is a supplementary service available from your service provider on ETSI ISDN BRI/PRI links. This feature allows the Business Communications Manager user to view the charges for an outgoing call once the call completes. This information is also reported to the Call Detail Reporting Application. The information can be provided in currency or charging units, depending on how the feature is set up by your service provider.

To invoke the feature, the user presses [✆] [8] [1] [8].

To set up MCID and network diversion, you can access the **Network Services** heading on the Unified Manager, as described in these steps:

1. Click the keys beside **Services**, **Telephony Services**, **General settings,** and **Network Services**.
2. Click on **ETSI**.
3. Table 86 lists the possible values for ETSI.

   The **Description** column of the table describes the feature and how the user activates each feature from their telephone.

Table 86 ETSI network values

Attribute	Values	Description
Netwrk Diversion	Y or N	Allows you to choose if you want to allow calls to be redirected to an outside network.
MCID	Y or N	Malicious Call Identification If you set this feature to Y, the called party can use ↻ 8 9 7 to request the network to record the identity of an incoming call. including: • called party number • calling party number • local time and date of the activity • calling party sub-address, if provided by the calling user
		Note: The feature code must be entered within 25 seconds of the caller hanging up (a 25-second busy tone occurs). If the called party hangs up first, there is no opportunity to use the feature. Note: The call identification comes from your service provider, not the Business Communications Manager. You must have the service activated by the CO before the feature is active for the user, regardless of the setting in this field.

DPNSS 1 Services

The Digital Private Network Signaling System (DPNSS 1) is a networking protocol enhancement that extends the private networking capabilities of existing Business Communications Manager systems. It is designed to offer greater centralized functionality for operators, giving them access to Business Communications Manager features over multiple combined networks.

Note: The DPNSS feature is dependent on which region loaded on your system at startup and that a software keycode was entered to enable the feature.

DPNSS 1 allows a Business Communications Manager local node, acting as a terminating node, to communicate with other PBXs over the network. For example, corporate offices separated geographically can be linked over DPNSS 1 to other Business Communications Manager nodes, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Business Communications Manager nodes to function like a private network, with all features of Business Communications Manager accessible.

Tips: Business Communications Manager DPNSS 1 works as a terminating node only. Business Communications Manager to Business Communications Manager DPNSS is not supported.

DPNSS 1 features can be used on any Business Communications Manager telephone. On most Business Communications Manager telephone, you must use specific keys and/or enter a number code to access the features. For a description of the types of Business Communications Manager telephone, see the *Business Communications Manager Telephone Feature Programming Guide*.

DPNSS 1 Capabilities

A single Business Communications Manager node, acting as a terminating node on the network, supports the following capabilities over DPNSS 1 lines:

- Direct Dial Inward (DDI) for incoming calls.
- Originating Line Identification (OLI) for incoming and outgoing calls:
  - For incoming calls, the Calling Line Identification (CLI/CLID) information is displayed to the user on telephone sets with line display This must be configured in programming.
  - For outgoing calls, the directory number of the originating party is sent out as OLI.
- Terminal Line Identification (TLI) for incoming and outgoing calls. Referred to as Called Line Identification.
- Selective Line Redirect (SLR) and External Call Forward (ECF) implemented on calls between DPNSS 1, and BRI/PRI, DASS2, and Analog lines.
- These remote access features are supported on DPNSS: DDI, line pool access code, destination Codes and remote page feature codes.

Software Keys are required to enable DPNSS 1.

DPNSS 1 Features

The following features are available and can be programmed over DPNSS lines:

- Three party service
- Diversion
- Redirection
- Call Offer
- Executive intrusion
- Route optimization
- Message waiting indication
- Loop avoidance

The following parameters can be configured for DPNNS 1 lines:

- Line type
- Prime set
- CLID set
- Auto privacy
- Answer mode
- Auxiliary ringer
- Full autohold

Some features are transparent to the user, but must be programmed to be activated. Others are available for end-user programming at the set. Detailed explanations of these features follows.

Three Party Service

Three Party Service is a DPNSS 1 feature for Business Communications Manager that is similar to the Business Communications Manager Conference feature.

The Three Party Service allows a user, usually an operator, to establish a three-party conference by calling two other parties from one telephone set. Once the connection is made, the controlling party can hang up, leaving the other two connected. The controlling party can even put one party on hold, and talk to the other party.

Note: Business Communications Manager does not support Hold over the DPNSS link itself. This means that the conferenced party on the distance end of the network cannot place a Three Party Service call on Hold.

This feature is basically designed to allow operators to assist in the connection of calls from one main location.

Making a Conference Call

To initiate or disconnect from a conference call on a Business Communications Manager system over DPNSS 1, use the procedure described in “Creating a conference call” in the Business Communications Manager Telephone Feature Programming Guide.

Note: Three Party Service is supported on M7000 telephone sets, but in a receive-only fashion. These set types cannot initiate Three Party Service. For more information about these set types, see the Business Communications Manager M7000 User Card.

Using the Diversion Feature

Diversion is a DPNSS 1 feature for Business Communications Manager that allows users to forward their calls to a third party on the DPNSS 1 network. This feature is similar to Call Forward on Business Communications Manager, but takes advantage of the broader capabilities of DPNSS.

There are five variations of Diversion: Call Diversion Immediate, Call Diversion On Busy, Call Diversion On No Reply, Bypass Call Diversion, and Follow-me Diversion. These variations are described below:

- Diversion Immediate diverts all calls to an alternate set. This function is programmed by the user at their telephone set.
- Diversion On Busy diverts all calls to an alternate set when a set is busy. This feature is programmed in the Unified Manager.
- Diversion On No Reply diverts calls that go unanswered after a specified amount of time. This feature is programmed in the Unified Manager.
- Bypass Call Diversion overrides all Call Forward features active on a set over a DPNSS line. An incoming call to the set will not be forwarded; instead, the set will continue to ring as if Call Forward were not active. This feature is used to force a call to be answered at that location. Bypass Call Diversion is a receive-only feature on Business Communications Manager, and cannot be used from a Business Communications Manager telephone.
- Follow-me Diversion is also a receive-only feature. It allows the Call Forwarded destination to remotely change the Business Communications Manager Call Forwarding programming (Call Forward All Calls (CFAC) feature) to a different telephone set.

Tips: Business Communications Manager CFAC must be active and the destination set/ PBX must support the feature.

For example, user A forwards all calls to set B, a temporary office. Later, user A moves on to location C. The user does not have to be at set A to forward calls to location C. Using set B and Follow-me Diversion, the user can forward calls from A to location C.

Follow-me diversion can be cancelled from the forwarded location.

Note: Diversion on Busy and Diversion on No Reply cannot be cancelled from the forwarded telephone sets. These are programmable only by an installer and not by the user.

Note: If multiple sets are programmed to take a call, the first set to respond will act. All other sets responding are ignored. Therefore, if the first set to respond has Diversion enabled, this feature will be invoked.

Restrictions by Telephone Type

- all variations supported on Business Communications Manager digital and IP telephones
- ATA—all variations supported on an ATA
- ISDN—all variations supported on ISDN telephones, except Diversion on Busy and CFWD Busy
- Portables—all variations supported on portable telephones

Setting Diversion

You set Diversion for DPNSS in the same way as Call Forward, see "Defining Capabilities" on page 157. You will need to enter the end DN when prompted. You may also need to include the DPNSS 1 routing number.

Using the Redirection Feature

Redirection is a DPNSS 1 feature similar to Business Communications Manager Transfer Callback. Redirection lets a call awaiting connection, or re-connection, be redirected by the originating party to an alternate destination after a time-out period. Failed calls can also be redirected. Priority calls are not redirected.

Note: The address to redirect depends on the history of the call. Calls that have been transferred are redirected to the party that transferred them. In all other cases, the address to redirect is the one registered at the PBX originating the redirection.

Note: Business Communications Manager does not support the redirection of Business Communications Manager originated calls, even over DPNSS 1.

The Diversion on No Reply feature takes precedence over Redirection.

Restrictions by Telephone Type

- For telephones without displays, the # key acts as MORE and the * key acts as VIEW
- ATA—not supported
- ISDN—all variations supported on ISDN telephones
- Portables—all variations supported on portable telephones

Setting Redirection

The timer used for the network Callback Feature is also used for redirection.

Executive Intrusion

Executive Intrusion (EI) is a DPNSS 1 feature that allows an operator, or other calling party, to intrude on a line when it is busy. An example of the use of this feature is to make an important announcement when the recipient is on another call.

EI is similar in functionality to Business Communications Manager Priority Call, but it is a receive-only feature on Business Communications Manager sets. EI cannot be initiated from a Business Communications Manager telephone. The person using this feature must be on another PBX on the DPNSS 1 network.

When EI is used to intrude on a call in progress, a three-way connection is established between the originating party and the two parties on the call. The result is very much like a conference call. When one of the three parties clears the line, the other two remain connected, and EI is terminated.

Restrictions by Set Type

- ATA—supported
- ISDN—not supported
- Portables—not supported

The set receiving the intrusion displays Intrusion Call. A warning indication tone will sound after intrusion has taken place, and the standard conference call tone will sound every 20 seconds.

Intrusion Levels

Whether or not a set will accept or reject an Executive Intrusion request depends on the level of intrusion protection programmed. Each set (DN) has an Intrusion Capability Level (ICL) and four Intrusion Protection Levels (IPL).

When the ICL of the intruding set is higher than the IPLs of *both* sets on the active call, EI will occur. It is best to set the IPLs of most the Business Communications Manager telephone to the default of **None**, or Low or Medium.

Intrusion levels are described as follows:

- ICL: determines the ability of the attendant to intrude. As long as the ICL is higher than the IPL of the wanted party, EI is allowed. Since EI is a receive-only feature, the ICL cannot be set on Business Communications Manager.
- IPL: determines the ability of the attendant to refuse intrusion. If the IPL is lower than the ICL of the originating party, EI is allowed. For general purposes setting the IPL to None, Low or Medium is recommended, unless intrusion is not wanted.

To program IPL on a telephone:

1. Click on the keys beside **Services, Telephony Services, System DNs, Active Set DNs, DN ##,** and **Capabilities**.
2. Choose **Intrusion**.
3. Click a **Protection level**: None, Low, Med, or High.

   If the level of intrusion protection is set to **High** no intrusions will be allowed. The default is **None**.

Call Offer

Call Offer over DPNSS 1 allows a calling party to indicate to the wanted party that there is an incoming call available, even though there is no answer button available to present the call on the set. The intended recipient can ignore, accept, or decline the offered call. Call Offer is useful in increasing the call-coverage capability of a Business Communications Manager system, and helps to lift the network processing load. It is a receive-only capability on Business Communications Manager: incoming calls would be initiated at another PBX on the DPNSS 1 network.

An example of Call Offer in use is an operator or attendant who has a number of calls coming in at once. The operator can call offer one call and move to the next without waiting for the first call to be answered.

Displays

When a Call Offer is made by the originating exchange, the target set displays a message, and a tone is heard. When an offered call arrives on sets with line display, the user sees `XX...X wtng` if the calling party ID is available and CLID is enabled. If CLID is not available or CLID is disabled, `Line XXX waiting` appears (the line name associated with the call). If there are more than 11 digits in the incoming number, only the last 10 will display.

If Call Queuing is programmed for the system, the display shows `Release Line XXX`.

This is the line name of the highest-priority queued call if it is an offered call.

Restrictions by Telephone Type

- M7000— associated LED or LCD flashes, and a tone is heard
- ATA—Call Offer is supported as a Camp On feature, and a tone is heard
- ISDN—not supported
- Portables—not supported

Note the following general conditions and restrictions:

- DND on busy must be programmed as N (**DN ##/Capabilities**) for a telephone to accept Call Offer.
- If CF on busy is programmed for the telephone, Call Offer is not accepted.
- The target line for the telephone must be set to: If **busy: busy tone**, which is the default. Refer to "Assigning Trunk/line Data" on page 97.
- Call Offer does not work if sent over Manual answer lines. It is recommended that the lines be left at the default: **Auto**.

User Actions

The party receiving a Call Offer has three choices:

- Ignore it. After a programmed time interval, the Offer request is removed.
- Reject it. If the user activates Do Not Disturb on Busy (DND) when the Call Offer request is made, the request is removed from the set. The calling party is informed of the rejection.

  A call cannot be offered to a set with DND active. The line indicator for external incoming calls still flashes.
- Accept it. The Offer is accepted by releasing the active call.

Note: Forward on Busy takes priority over DND on Busy. Call Offer cannot be accepted by putting an active call on hold.

Route Optimization

Route Optimization is a DPNSS 1 feature for Business Communications Manager that lets calls follow the optimum route between two end PBXs. This allows efficient use of network resources.

Route Optimization is initiated by the system and is transparent to the user. However, the user may see a call switch from an appearance on the set to another appearance key or from an intercom key to the appearance key or vice versa. This occurs when Business Communications Manager receives a Route Optimization request and initiates a new call to follow the optimal route.

If a set is active on a private line call, the Route Optimization call being established may go on a public line. This will cause a loss of privacy on that line.

Data calls are rejected by Route Optimization in order to ensure the data transmission is not affected.

Certain situations result in Route Optimization not taking place. For example, calls that are using Hold, Parking or Camp features do not undergo Route Optimization, and if a Route Optimization call undergoes Diversion, the Route Optimization is dropped.

Setting Route Optimization

There is no system programming required for the feature when Business Communications Manager is working as a terminating PBX. However, Business Communications Manager must have a private access code programmed that maps to a valid destination code or line pool code on DPNSS lines. Further, Allow redirect must be set to **Y**. For more information, see "Defining Capabilities" on page 157.

Message Waiting Indication

Message Waiting Indication (MWI) is a DPNSS 1 feature for Business Communications Manager Call Services. Messages are received at a centralized location, to a pre-determined telephone, where they are processed and forwarded to the target set. This centralization relieves the network processing load, making the system more efficient. MWI provides users with the ability to scroll through, erase and reply to messages.

When there are messages to retrieve, `Message for you` appears on the telephone display. After all the messages are retrieved by the user, a Message Waiting Cancellation (MWC) is sent from the call center, and the user set no longer displays an MWI message.

MWI allows the user to reply or call back to the message center. The procedure for retrieving messages is described in the Business Communications Manager Telephone Feature Programming Guide.

This feature is only supported on Business Communications Manager target lines.

Restrictions by Set Type

- M7000—associated LED flashes
- ATA—not supported.
- ISDN— not supported.
- Portables—not supported.

Setting Message Waiting Indication

To set Message Waiting Indication:

- Assign message center to a line.
- Select message center for use.
- Assign the line to a set to Appear and/or Ring.

Assigning Message Centers to a Line

You need to assign any one of five, or None, of the message centers to the line. There can be as many as five message centers in a network; that is, five telephone sets on the Business Communications Manager system can act as mailboxes in the message centers offered by five different PBXs on the network. These PBXs may also be from different manufacturers.

Thus, for each message center there may be different:

- numbers to be dialed to reach the mailbox from the set
- MWI strings received, indicating that the center has a message in the mailbox
- MWC strings received, indicating that the voice mails have been retrieved

When assigning message centers, you can program all three parameters for each. Remember that the following procedure is not to select a message center, but to program any or all of the five available message centers. This is similar to the Direct Dial functionality.

Tips: The MWI and MWC strings used in this procedure are default NSI strings for Message Waiting.
*58B*AN*1# – Message Waiting Indication
*58B*AN*0# – Message Waiting Cancellation
This provides the information required to program the strings as:
AN*1# for MWI, and
AN*0# for MWC
Private network strings will differ with different message centers. These should only be changed on the advice of your customer service representative.

---

1. Click the keys beside **Services**, **Telephony Services**, **Lines,** and **Telco Features**.
2. Click **Voice message center numbers**.
3. Choose a Voice message center: **1** to **5**.

   The existing telephone (DN) for Message Waiting appears if available, as **Tel#:XXXX**.
4. Type the new target number, starting with an access code, if required, or **None**. For example: **65142222**.

   The display shows **MWI:AN*1#**. This is a string sent by the PBX holding the message center.
5. Program the number that the user will dial on the IC key to retrieve a message from the messaging center.

6 Program the Non-Specified Information (NSI) string for the MWI that is expected from the particular message center.

The display shows **MWC:AN*0#**. See the next procedure: "Programming MWI and MWC".

7 Program the NSI string for the MWC that is expected from the message center.

Note: The line must be programmed to Appear and/or Ring at the set.

Programming MWI and MWC

MWI and MWC information is received from the network in the form of NSI strings. The NSI strings in DPNSS are dependent on the supplier of the PBX. Therefore, the strings vary depending on the originating PBX.

Each string has the following default structure: *58XYYYYY.*

Table 87 describes each part of the NSI string:

Table 87 Parts of the NSI string

String Component	Description
*58	Identifies that it is an NSI string.
X	Any letter from A to Z, or nothing.
YYYYY..	Manufacturer specific string, which can contain any sequence of alphanumeric digits or *.
#	Marks the end of the identifier.

Only the YYYYY.. # portion of the string must be programmed for MWI and MWC. The procedure is similar to Set Name/Line Name.

The following criteria must be met when programming NSI strings for MWI/MWC:

- No spaces are allowed, including spaces at the end of the string.
- A # must be present at the end.
- A # or a * cannot be present in the first character.

Selecting a Message Center

With a message center programmed on a selected line, you must set the message center for use:

1 Click the keys beside **Services**, **Telephony Services**, and **Lines**.

2 Click a target line number (Line 241 to 364).

3 Click the key beside **Telco Features**, then click on **Voice message center numbers**.

4 Choose a Voice Message center: **1** to **5**.

Setting Message Waiting Indication

Follow these steps to set the MWI:

1. Ensure that you have programmed a set to access target lines for receiving messages. For information on access to target lines, refer to "Assigning Message Centers to a Line" on page 242
2. Click on the keys beside **Services**, **Telephony Services**, **System DNs**, and **Active Set DNs.**
3. Click a DN (DN 221-528).
4. Click on the key beside **Telco Features**, and select **Feature assignment**.
5. Click **Y** to enable Call log set.
6. Click **Y** to enable Vmsg set.

   When Vmsg is enabled for a target line on a set, the set logs Message Waiting Indication/ Cancellation received for the corresponding target lines to the user.

Loop Avoidance

Errors in the configuration of a network may make it possible for a call to be misrouted, and arrive at a PBX through which it has already passed. This would continue, causing a loop which would eventually use up all of the available channels. The Loop Avoidance service permits counting of DPNSS 1 transit PBXs and rejecting a call when the count exceeds a predetermined limit.

Programming Loop avoidance

To set Loop avoidance during hardware configuration:

1. Click the keys beside **Resources, Media Bay Modules**, **Bus 02 - 07**, **Modules on Bus.**
2. Select **Module 1.**
3. Choose **Module type DPNSS**.
4. Type a value (0-25) in the Maximum transits box.

   The default value is 25.

Private Networking with DPNSS
(International only)

DPNSS supports the Universal Dialing Plan (UDP), an international standard for sending and receiving private numbers over networks. The UDP requires that a dialing number includes the following:

- a Private Access Code, programmed into the system as part of the destination code table to prevent conflicts with the internal numbering system. (**Access Codes**)
- a Home Location Code (HLC) assigned to each PBX, and configured as part of the destination code (a maximum of seven digits). For each HLC, a routing code must be programmed in the system. (**Dialing Plan/UDP/Location code**.)
- a Directory Number (DN) assigned to each extension as a line appearance. The DN appears as the last string segment in a dialed number. In the number 244-1111, 1111 is the DN.

A typical Private Number, using a Private Access Code and dialed from another site on the network, appears below.

Private Access Code	+ Home Location Code	+ Directory Number	= Calling Party Number
6	+ 848	+ 2222	= 6-848-2222

In this networking example, a private network is formed when several systems are connected through a Meridian M1 and a terminating Business Communications Manager system. Each site has its own HLC and a range of DNs. Figure 45 on page 246 illustrates this example.

Calls are dialed and identified to the system as follows:

- To reach a telephone inside the Private Network, at the Business Communications Manager site, the user dials the DN of choice.
- To reach a telephone inside the Private Network, from another site, the user dials HLC + DN.
- To reach a set outside the Private Network, the user dials an Access Code + HLC + DN

  Each node has its own destination (dest) codes which includes the appropriate access and HLC codes to route the call appropriately.

Table 88 shows examples of the construction of numbers used when dialing within the example network. Note that 6 is the Private Access code.

Table 88 Calling numbers required for DPNSS network example

Calling Site	LOC/HLC	Calling Party Number	Called Site	Dialling String	Called Party Number
Site A	244	244 1111	Site B	6 668 2222	668 2222
Site B	668	668 2222	Site D	6 848 2222	848 2222
Site D	848	2222	Site D	2229	2229
Site C	496	496 3333	Public DN	9 563 3245	563 3245

Figure 45 DPNSS networking

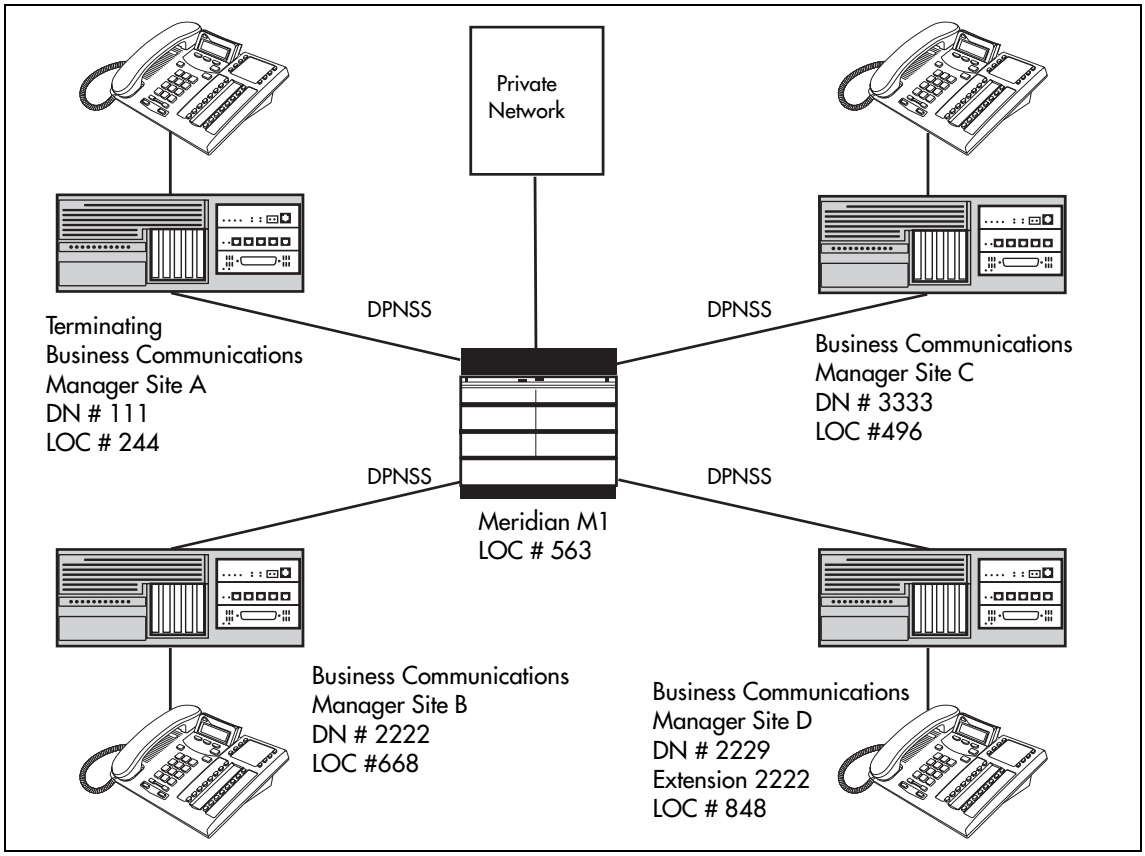


Table 89 shows examples of the routing required to set up the network shown in Figure 45 on page 246. Note that 6 is the Private Access code.

Table 89 Routing for DPNSS network

Heading	Parameter	Setting	
Private Network: (for each branch Business Communications Manager)			
Routing service to		Private network	Public network
	Route	001	002
	Dial out #	No number	No number
	Use	Pool N	Pool N
	DN type	none (private access code 6 is programmed)	public
	Destination Code	6	9
	Normal route	001	002
	Absorb	1	1

For more information on creating a private numbering plan with DPNSS, refer to:

- "Guidelines for Creating a Private Numbering Plan with DPNSS" on page 247
- "Customizing the Routing Service" on page 247

Guidelines for Creating a Private Numbering Plan with DPNSS

Use the following guidelines when creating a private numbering plan with DPNSS.

- When creating HLCs for the nodes in your system, avoid numbering conflicts between network nodes and internal DNs, Hunt Group DNs.
- Program a Private Access Code into your dest routing tables to avoid conflicts with your internal HLC and dest code numbering plan. For example, if a dialout HLC is 848, but this number already exists in the Business Communications Manager system for an extension, the routing tables should add a Private Access Code to the dest code. If the code is programmed as 6, the dest code becomes 6848. 6848 uses a route to dial out 848 using the DPNSS line pool, allowing the call to be placed.

  Note that a Private Access Code is required only for specific DPNSS features such as Diversion, Route Optimization, and Redirection.

Customizing the Routing Service

You can customize the routing service using the following restrictions:

- Direct Inward Access (DIA) lines allow incoming calls on private circuits to be directed to telephones without going through the normal call reception. Each DIA line is assigned to one or more extensions and is given a distinct Private Received number. When someone on another system on the network dials the Private Received number on a DPNSS line, the Business Communications Manager system checks all received digits, compares the digits to an internal table and routes the call to the appropriate DIA line. All extensions programmed to have access to that DIA line will then alert for the incoming call.
- Dialing restrictions can be added to lines in line pools. Filters can restrict the use of the line to specific area codes.
- Host system signaling codes can be part of the dial out for a route. Routing can also be used as an alternate method for a direct-dial number. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Digit absorption should be set to 1. Because overflow routing directs calls using alternate line pools, a call may be affected by different line restrictions when it is handled by overflow routing.

VoIP Networking

When you choose voice over IP (VoIP) trunks to make network connections, the process is very much the same as using PRI SL-1 lines, except that you must also create a Destination Gateway record, which identifies the IP address for the target system. For detailed information about setting up IP networks, refer to the *IP Telephony Configuration guide*.

Tips: MCDN currently is not available over VoIP network lines.

Chapter 11
Configuring System Settings

This chapter describes the headings where you configure system-wide settings.

Scheduled Services Headings

The Scheduled Services headings access records that allow you to define service by the time of day and day of week for the following services:

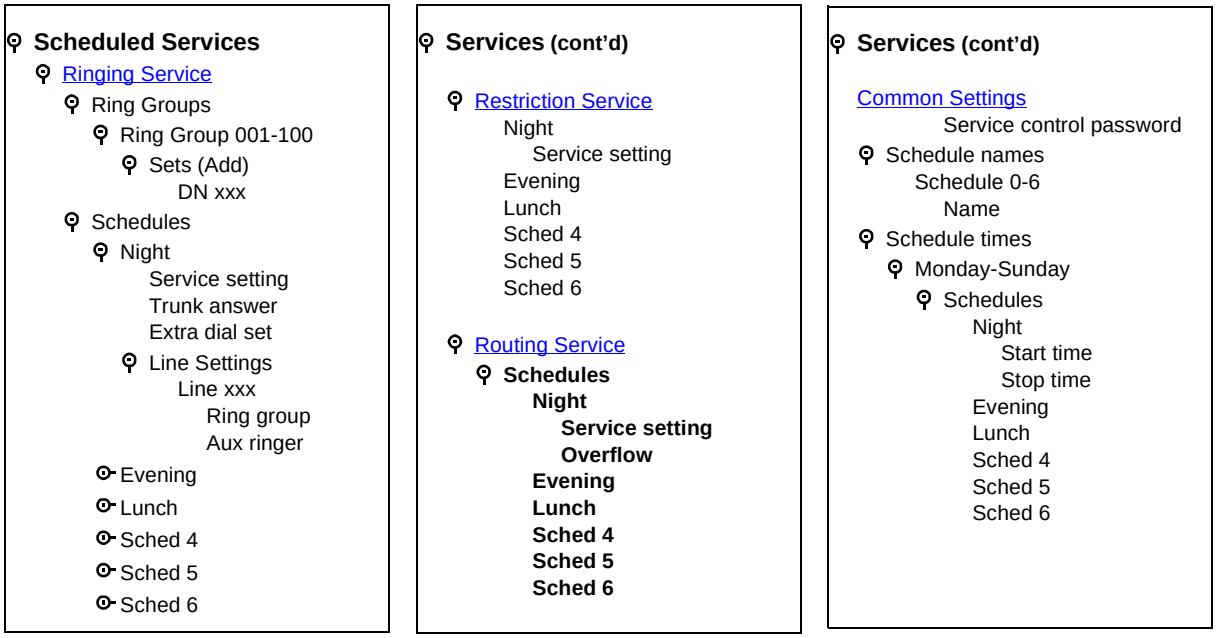
- ringing
- restriction
- routing

The Common Settings headings allow you to determine the schedule names and times for the scheduled services.

Note: To use scheduled services, you must define a Control set for the set you want to use schedules with. Control sets are defined in the DN records under **System DNs**.

Figure 46 shows the Scheduled Services navigation tree headings:

Figure 46 Scheduled Services headings



Common Settings

The **Common Settings** heading allows you to define the common names and times for the services schedules. You also define the service control password under this heading.

Defining the Service Control Password

Use these steps to locate and confirm or change the password the user will need to access the service feature from a telephone.

1. Click the keys beside **Services**, **Telephony Services**, **Scheduled Services.**
2. Click on **Common settings**.
3. In the **Service control password** field, the default is set at 23646. You can change this, as required.

Tips: Users need this password to allow them to change Restriction or Routing service settings on a control telephone.

Changing Schedule Names

Schedules have been given default names, however, if you change the purpose of your schedules, you can also change the name to reflect their purpose.

For example: If you have VoIP trunks on which you want to allow fallback to a ground trunk, you must define a 24-hour schedule for the preferred VoIP trunk destination code.To do this, you can rename schedule 4, 5, or 6 to Sched VoIP, so that you know which schedule to use when you are assigning the feature to telephones.

Use these steps if you want to change the name of a schedule.

1. Click on the **Common Settings** key and on the **Schedule Names** key.

   A list of seven schedule records displays.

Note: Schedule 0 is named Normal and cannot be changed.
Schedule 1 to 6 have default names which can be changed to meet your requirements.
Refer to the *Telephone Features Programming Guide* for instructions about how to activate schedules on the telephone, and how to display the schedule name that is currently running.

2. Click on the **Schedule** you want to change the name for.
3. Type in a new name for the schedule, then press <Tab> to save the change.

Tips: Reserve a couple of schedules (i.e. 4, 5, and 6) for alternate call routing, such as for VoIP trunk routing.

Schedule Times

Schedule start and stop times are set at times you are most likely to want each service to be active.

1. Click the keys beside **Services**, **Telephony Services**, and **Scheduled Services,** and **Schedule times**.
2. Click the key beside the day you want to program (for example, **Monday**).
3. Click the key beside **Schedules**. The programming menu expands to display all the schedules.
4. Click the schedule you want program. The Day-Schedule window appears.
5. Type the start and stop times for each schedule, on each day.

   Table 90 provides a list of the default times for each schedule.

Table 90 Default schedule times

Schedule	Start time	Stop time
Schedule 1: Night	23:00	07:00
Schedule 2: Evening	17:00	23:00
Schedule 3: Lunch	12:00	13:00
Schedule 4: Schedule 4	00:00	00:00
Schedule 5: Schedule 5	00:00	00:00
Schedule 6: Schedule 6	00:00	00:00

About Start and Stop Times

Here are some general rules about setting start and stop times:

- It is only necessary to program start and stop times for schedules that are activated automatically. See the instructions with Ringing service for information on activating schedules.
- The time may be entered in either 12 or 24-hour format. If the display is in English, and the hour entered is less than 13, the display prompts you to specify **AM** or **PM**.
- If you assign identical start and stop times for a schedule, for example, 04:00 start and 04:00 stop, the schedule is in effect all day. The only exception to this is a start and stop time of 00:00; in this case the schedule is off for the day.
- You may assign overlapping times. For example, if schedule 1 is assigned from 9:00 am to 4:00 pm and schedule 2 is assigned from 1:00 pm to 5:00 pm, then the start time of the second schedule is treated as a stop time for the first schedule.
  This is also true if two schedules have the same start time but different stop times; the stop time of the shorter schedule is treated as the start time of the longer schedule.
- If one schedule starts and stops within the times of another schedule, the first service temporarily ends when the second service starts. The first service then resumes when the second service has ended.

- Some schedules start and stop at the same times each day: use **COPY** to copy the start and stop times from one day to the next.

Warning: Start and stop times do not span days.
When you program a schedule to start in the evening and stop in the morning, it does not carry over into the next day. For example, if you program Night service for Friday (22:00 to 6:00), the system turns on Night service from midnight to 6 am on Friday, and then again from 10 pm to midnight on Friday.

Programming Scheduled Services

Each of the three services has six schedules that you can customize.

For example, you may want to combine alternate call ringing with alternate dialing restrictions for lunchtime, evenings, and weekends (Schedules 1, 2, and 3). Then you may want to run alternate call routing using three separate schedules.

Tips: Once you have programmed the different services and schedules, you can turn each of the services on separately. For example, the Night schedule might control both Ringing service and Restriction service. But you can turn on just the Ringing service part of the Night schedule if you wish.

You can activate the services from the designated control telephone for each telephone and line in your system.You can have one control telephone for the whole system, or different control telephones for different telephones and lines.
If you want to have several services active at the same time, simply program them on for the same schedule.

Note: To program services from a telephone, you require an access code.

Ringing Service

At certain times or in certain situations, you may want additional telephones to ring for incoming lines. The most common use of this feature is when a security desk telephone rings for incoming lines after 5:00 p.m., a practice often called *night service*.

Ring Groups

Ring groups allows you to define groups of extended ringing sets. A group can be assigned to any line for any of the schedules. You can define up to 100 ring groups with up to 30 sets for each ring group.

1 Click the keys besides **Services**, **Telephony Services**, **Scheduled Services**, **Ringing service**, and **Ring groups**.

A list of ring groups displays.

2 Click the key beside the ring group you want to program. The subheading **Sets** appears.

3 To add DNs, click on **Sets**, and then click the **Add** button, located at the top of the column.

4 In the Add Sets window, type the DN of the set you want to assign to this ring group.

Tips: You can assign any set on the Business Communications Manager system to a ring group. The assigned control set for each schedule is added to each ring group.
A set can belong to more than one ring group.

5 Click **Save** to enter the DN.

6 Repeat steps 4 to 6 until you have added all the sets you want.

Schedules

Indicate how Ringing service should be activated for each of the schedules:

1 Click the keys beside **Services**, **Telephony Services**, **Scheduled Services**, **Ringing service**, and **Schedules**.

2 Click a schedule name (for example, **Night**). The window for that schedule appears.

3 Table 91 shows the possible settings for each schedule day.

Table 91 Schedule values

Attribute	Value	Description
Service setting	Off Manual Auto	**Manual** allows you to turn the service on and off at any time from a control set using the Ringing service feature code. **Auto** allows you to program a stop and start time for a service. You are still able to start and stop the service by entering the appropriate Services feature code at a control set. If you select this setting, you will have to set start and stop times. See "Schedule Times" on page 251 for information on programming times. **Off** prevents the service from being activated.

Table 91 Schedule values (Continued)

Attribute	Value	Description
Trunk answer	Y or N	Trunk answer allows you to answer, from any telephone, an external call that is ringing at another telephone in your office if the Ringing Service is active on that line at the time of the call. If the service is not active, you cannot answer the call. This is useful if the other telephones are not assigned the same lines as the telephone you are using to answer the call.
		Note: You can change the Trunk Answer setting only if Ringing service is set to Manual or Automatic.
Extra dial set	None DN XX DN <control set>	The Extra dial set attribute allows you to assign an additional direct-dial set for each schedule.
		Note: The extra dial set is activated during a schedule by entering the Ringing service feature code from a direct-dial set. This does not activate the Ringing service unless the direct-dial set is also a control set.

Line Settings

Each line must be assigned a Ringing service for ring group and auxiliary ringer.

Note: If the lines are not set up yet, skip this step until you have defined all the lines.

1 Within each ring schedule name, click on the key beside **Line settings** to display the list of lines.

2 Click on each line in turn, or a specific line you want to adjust.

3 Figure 92 shows the possible settings for each schedule day.

Table 92 Schedule values

Attribute	Value	Description
Ring group	Ring group XXX	Type in a ring group number (001-100) to choose a different ring group assignment. Only one ring group can be assigned to a line for each schedule. To combine groups of ringing sets, you must create a new ring group which contains all the sets you want to ring and assign it to the line.
Aux ringer	Y or N	This variable indicates whether the auxiliary ringer (if installed) also rings when Ringing service is on.

Table 92 Schedule values (Continued)

Attribute	Value	Description
		Tips: • The default ringing telephone is 221. This means that all lines ring at telephone 221 when Ringing service is on. • You can copy Ringing set and Auxiliary ringer programming from one line to another. • If you have an auxiliary ringer programmed to ring for calls on an external line and you transfer a call on that line without announcing the transfer, the auxiliary ringer will ring for the call transfer.

Restriction Service

Use these commands to indicate how the alternate dialing restrictions become active for each schedule.

1 Click the keys beside **Services**, **Telephony Services**, **Scheduled Services,** and **Restriction service**.

2 Select the schedule you want to program, (for example, **Night**).

The schedule window appears.

3 Table 93 shows the possible settings for each schedule day.

Table 93 Schedule values

Attribute	Value	Description
Service setting	Off Auto Manual	**Manual** allows you to turn the service on and off at any time from a control set using the Ringing service feature code. **Auto** allows you to program a stop and start time for a service.You are still able to start and stop the service by entering the appropriate Services feature code at a control set. If you select this setting, you will have to set start and stop times. See the section on schedule times for information on programming times. **Off** prevents the service from being activated.

Tips: This service requires a Service Control Password to use. Users obtain this password from their system coordinator.

Refer to "Defining the Service Control Password" on page 250.

Routing Service

The Routing service command allows you to set activate routing tables for each of the schedules.

1. Click the keys beside **Services**, **Telephony Services**, **Scheduled Services**, and **Routing service**. Schedule names display.
2. Select the schedule you want to program, for example, **Night**. The schedule window appears.
3. Table 94 shows the possible settings for each schedule day.

Table 94 Schedule values

Attribute	Value	Description
Service setting	Off Auto Manual	**Manual** allows you to turn the service on and off at any time from a control set using the Ringing service feature code. **Auto** allows you to program a stop and start time for a service. You are still able to start and stop the service by entering the appropriate Services feature code at a control set. If you select this setting, you will have to set start and stop times. See the section on schedule times for information on programming times. **Off** prevents the service from being activated.
Overflow routing	Y or N	If all the lines used by a route are busy when a call is made, you can program Routing service to overflow to the route used for normal mode. If this happens, the set sounds a warning tone and displays the message **`Expensive route`**. The caller can then release the call to avoid using the normal route, or continue with the call.
		Tips: A schedule must be active for overflow routing to be in effect. Overflow routing is not available in normal mode. You must create an overflow route to be used with each destination code. In this way, every route used with a scheduled mode that has overflow service must have an alternate route in normal service.

Tips: This service requires a Service Control Password to use. Users obtain this password from their system coordinator.

Refer to “Defining the Service Control Password” on page 250.

Services Matrix

To help you with your services planning, transfer the following information to a spread sheet and fill out the values for each type of service.

Table 95 Ringing and Scheduling Services

Ringing Services	
Ring grp #	Sets

Scheduling Services		
Schedule	1 2 3 4 5 6	
Ctrl set:	221	
Service setting	Off Auto Manual	
Trunk answer	Y N	
ExtraDial	221	
Line settings		
Line #	Ring group (name)	Aux ringer
		Y N

Table 96 Restriction and Routing Services

Restriction Service	
Schedule	1 2 3 4 5 6
Service setting	Off Auto Manual

Routing Service	
Schedule	1 2 3 4 5 6
Service setting	Off Auto Manual
Overflow	Y N

Table 97 Common settings: Schedule Name

Common settings: Service control password		
Schedule Name		
Schedule 0	Normal	
Schedule 1	Night	
Schedule 2	Evening	
Schedule 3	Lunch	

Schedule 4	Sched 4	
Schedule 5	Sched 5	
Schedule 6	Sched 6	

Table 98 Common settings: Schedule times

Common settings: Service control password
Schedule Times

Table 98 Common settings: Schedule times

Monday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time
Tuesday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time
Wednesday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time
Thursday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time
Friday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time
Saturday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time

Table 98 Common settings: Schedule times

Sunday	Schedule: 0 (Normal) 1 2 3 4 5 6	Start time	Stop time

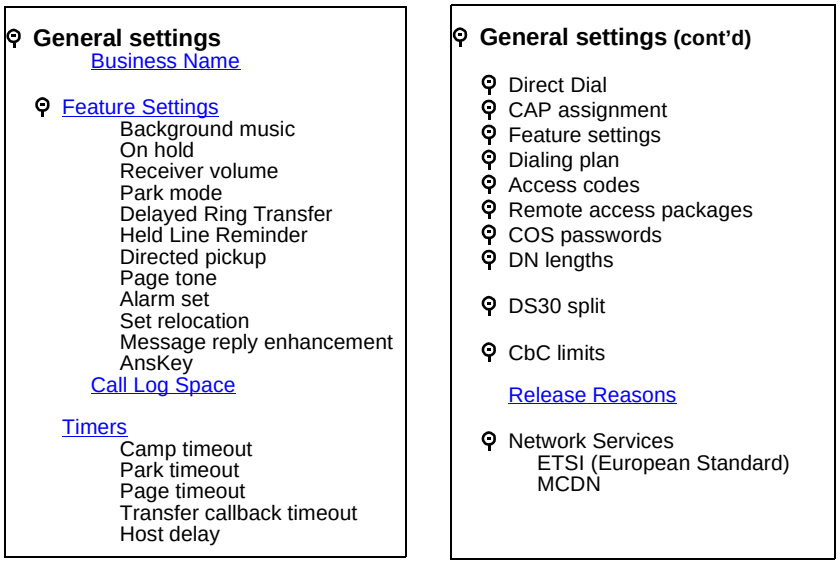
General Settings

The General Settings headings allow you to define several types of system-wide settings. This section includes settings that do not affect the call process, which are discussed in other areas of this book.

The commands that deal with restricting or controlling the call process are discussed in "Controlling Access to the System" on page 175.

Figure 47 lists the General Settings headings discussed in this section.

Figure 47 General Settings headings and fields



Business Name

The name you enter beside Business name will display on the telephone of the person you call. If you leave this field blank, nothing will display.

1. On the navigation tree, click on the keys beside **Services**, **Telephony Services**.
2. Click on **General Settings**.

   The General settings screen appears in the right frame.
3. In the **Business Name** field, type up to seven characters, and then press <**Enter**>.

Feature Settings

The Feature settings heading allows you to program a number of features that apply to all telephones connected to Business Communications Manager.

Follow these steps to define feature settings on a specific telephone:

1. On the navigation tree, click on the keys beside **Services**, **Telephony Services**, and **General Settings**.
2. Click on **Feature settings**.

   The Feature Settings screen appears in the right frame.
3. Use the values in Table 99 to set the features you have on your system.

Table 99 Set feature values

Attribute	Value	Description
Background music	Y or N	Allows you to listen to music through your telephone speaker after pressing F86 on your set. A music source must be connected to Business Communications Manager.
On hold	Tones Music Silence	Allows you to choose what a caller hears on an external line when the line is put on hold. Tones provides a periodic tone. Music provides any signal from a source such as a radio connected to Business Communications Manager. Silence provides no audio feedback.
Receiver volume	Use sys volume Use set volume	Allows you to specify if the volume level of a receiver or headset returns to the system default level when a call ends or is put on hold, or if it remains at the volume level set at the individual telephone.
Park mode	Lowest Cycle	The Call park feature allows you to suspend a call. It also allows someone to retrieve the call by entering a retrieval code at any telephone in the system. Park mode is the setting that determines how the system assigns a retrieval code to parked calls. When set to **Lowest**, the system chooses the lowest code that is available when the call is parked. When set to **Cycle**, the system will choose the codes in a sequence, from lowest to highest, until all the codes have been used.

Table 99 Set feature values (Continued)

Attribute	Value	Description
Delayed Ring Transfer	1, 2, 3, 4, 6 or 10	Defines whether unanswered external calls are automatically forwarded to a prime telephone after a certain period of time. You must assign a prime telephone for this feature to operate. Assign a prime telephone to one or more external lines in **Line Data** programming.
Held line reminder	Off After 30, 60, 90, 120, 150 or 180 Seconds	Reminds you that a call at your telephone is still on hold. You periodically hear two tones from your telephone until you return to the call on hold. Choose the number of seconds before the Held line reminder feature begins at a telephone that has an external call on hold.
Directed pickup	Y or N	Allows you to answer any calls by specifying the ringing telephone internal number. Directed pickup is useful when not all the telephones have the same lines, but you want to allow co-workers to answer a call on any external line from their telephones. **Note:** Do not confuse Directed pickup with the Group pickup feature. Group pickup, allows you to answer a call at any telephone within a specific group without specifying the internal number of the ringing telephone.
Page tone	Y or N	Defines whether a tone sounds before a page begins.
Alarm set	None DN: <number>	Allows you to assign a telephone on which alarm messages appear when a problem has been detected in the system. Alarms are recorded in the Windows NT event log.
Set relocation	Y or N	Allows you to move any telephone to a new location without losing the directory number, autodial settings, personal speed dial codes, and any programming for that telephone. Activate Set relocation after you do the set installation and programming, for more flexibility in testing equipment. If you deactivate Set relocation while moving a set, the internal number and programming data remain with the physical port on Business Communications Manager. When you connect the set somewhere else, it does not receive the original programming. Change this attribute to N once the set has been moved.
Message reply enhancement	Y or N	The Message reply enhancement feature allows you to automatically deactivate the message waiting indicator on analog telephones connected to an Analog Station Media Bay Module (ASM), if the reply call from the analog telephone to the direct-dial telephone is answered. It does not matter where the call is answered from by the user. This feature also functions if the user invokes the Call pickup feature to answer the reply call from the analog set. It does not however, work with the Retrieve parked call feature.
		Tips Direct-dial sets are the only sets that can send messages (using F1) to analog telephones connected to an ASM. The direct-dial set must be the designated direct-dial set for the analog telephone receiving a message.

Table 99 Set feature values (Continued)

Attribute	Value	Description
Ans key	Basic, Enhanced, or Extended	There are up to eight answer keys that you can assign to a set. The **Answer key** setting in **Feature settings** window allows you to determine what types of calls alert at the telephone. Answer key changes do not apply to portables. Refer to Table 100 on page 262 for attributes of each setting.
*Conference Tone	Yes or No	This setting determines whether a conference tone is heard by participants at the beginning of the conference. *Available only for selected regions.
*Network Callback Timer		This timeout value determines when a transfer attempt will stop and then attempt a retry of the transfer. *Available only for selected regions.

Table 100 shows the three Answer key levels.

Table 100 Answer keys

Answer keys	Basic	Enhanced	Extended
All calls except	X	X	X
Prime set call capture		X	X
Call forwarded calls			X
Other answer key calls			X
Priority calls			
Voice calls			
Ringing service			X
Callbacks			X
Line transferred calls			X

Phantom DNs

A Phantom DN is a set record for a set that does not physically exist. You can assign lines to the set that can be programmed to Appear and Ring. This allows you to assign an Answer key from the non-existent set to an existing set. This might be used in the case where a customer number has been changed, but the number still get used. Rather than assign a set, you can create a phantom DN and assign an Answer key to an active set.

SWCA Controls

The system-wide call appearance (SWCA) feature displays call appearances on any telephones that have buttons assigned for SWCA answer keys. The SWCA controls provide you with the ability to determine how you want the system to handle calls that come into telephones with defined SWCA buttons.

Follow these steps to set the SWCA controls for your system:

1. On the navigation tree, click on the keys beside **Services**, **Telephony Services**, **General Settings**, and **Feature settings**.
2. Click on **SWCA Control**.

   The SWCA Control screen appears in the right frame.
3. Use the values in Table 101 to set the SWCA controls.

Table 101 SWCA control values

Attribute	Value	Description
Auto-Assign call button	Y or N	If set to Yes, the SWCA feature automatically associates a new incoming call to an available SWCA button on any telephones in the system that have SWCA buttons assigned. If set to No, the user must press an available SWCA button to assign an incoming call. This can be done for both incoming and outgoing calls. The call then appears on all telephones with SWCA buttons assigned. Refer to "Programming Telephone Buttons" on page 163.
Invoked by Hold	Y or N	If set to **Yes**, a call assigned to an SWCA button follows the SWCA hold protocol. This means that if an active call is put on hold at one telephone, all telephones with that SWCA call appearance will show that the call is on hold, and can be picked from another telephone. The indicator flashes fast on the telephone where the call is put on hold. The indicator flashes slowly on all other telephones with an active SWCA button. If set to **No**, a call assigned to a SWCA button follows the normal telephone hold protocol. The call holds on the set where the call was answered or originated, and cannot be picked up by other users. Also refer to "Auto hold" on page 157.

How SWCA works on the telephone:

You have six SWCA call buttons set up on a telephone, and the telephone has been set to auto-assign call buttons.

When a call comes in, or if you make a call, the call is automatically assigned to the first available SWCA call button. As well, the call appears on all other telephones that have the same SWCA call button assignment. This frees up the incoming/outgoing line for the next call. As long as the first call is active or on hold, the next call coming in will be assigned to the next SWCA call button, and so on, until all six buttons are full. Any call coming in after this point remains on the main line, assuming no call buttons become free.

Note: Intercom keys do not interact with this feature.

Call Log Space

The Call log space heading allows you to reallocate the Call log space equally to all telephones in your system.

Warning: Use this heading only if you want to allocate an equal amount of log space to all the telephones in your system.
Reallocating Call log space may destroy Call log data at telephones that lose space. There are 600 Call log spaces available in the system. There are no spaces allocated by default. Changing the space allocation using Log defaults defines the log space available to all telephones in the system.

To reset call log space, follow these steps:

1. Click the keys beside **Services**, **Telephony Services**, **General settings**, **Feature settings.**
2. **Click on Call log space**.
3. On the menu at the top, click Configuration.
4. Click **Reset logs**.

   The Property sheet window appears.
5. Type the space allocation for the Call log at each telephone.
   a. In the **Space per log** box of the Property sheet window, type a three-digit number (for example, 020, to give each set 20 spaces).
   b. In the **# of sets with logs** box in the Property sheet window, type the number of sets with logs.
6. Click **OK**. The system automatically reallocates log space.

System Features Matrix

To help you identify your system feature settings, transfer the following information to a spread sheet and fill out the values.

Table 102 System features

Background music	Y or N
On hold	Tones Music Silence
Receiver volume	Use sys volume Use set volume
Park mode	Lowest or Cycle

Page tone	Y or N
Alarm set	None DN: DN <control set>
Set relocation	Y or N
Message reply enhancement	Y or N

Table 102 System features (Continued)

Delayed Ring Transfer	1 2 3 4 6 10
Held line reminder	Off 30 60 90 120 150 180 seconds
Directed pickup	Y or N

Answer key	Basic Enhanced Extended
Conference Tone	Y or N
Network Callback Timer	

Timers

The Timers heading allows you to define a number of timer settings for your Business Communications Manager system. These settings apply to all telephones connected to the Business Communications Manager system.

1 Click the keys beside **Services**, **Telephony Services**, and **General Settings**.

2 Click on **Timers**.

The Timers window appears in the right frame.

3 The possible settings are described in Table 103.

Table 103 Timer values

Attribute	Values	Description
Camp timeout	30, 45, 60, 90,120, 150 or 180 seconds	Allows you to assign the number of seconds before an unanswered camped call returns to the telephone that camped the call.
Park timeout	30, 45, 60, 90, 120, 150, 180, 300 or 600 seconds	Allows you to assign the number of seconds before a parked call on an external line returns to the originating telephone.
Page timeout	15, 30, 60, 120, 180, 300, 600 2700 seconds	Defines the period of time after which the paging feature automatically disconnects.
Transfer callback timeout	3, 4, 5, 6 or 12	Allows you to specify the number of rings before a callback occurs on a transferred call. You can estimate the delay in seconds if you multiply the number of rings by six. Note: This setting can affect transferred calls from voice mail and should be configured accordingly.
Host delay	200, 400, 600, 800, 1000, 1200, 1400, 1600, 1800 or 2000 milliseconds	Assigns the delay between the moment an outgoing line is selected to make an external call (for example, by lifting the receiver off the telephone) and the moment that Business Communications Manager sends dialed digits or codes on the line.This ensures that a dial tone is present before the dialing sequence is sent. Minimizing this delay provides faster access to the requested features.
Link time	100, 200, 300, 400, 500, 600, 700, 800, 900 or 1000 milliseconds	Allows you to specify the duration of a signal required to access a feature through a remote system. The Link time depends on the requirements of the host switching system. For example, to program external dialing through a Centrex system requires a Link time of 400 ms. Link is another name for recall or flash.

Timers Matrix

To help you identify your system timing settings, transfer the following information to a spreadsheet and fill out the values.

Table 104 Timer values

Camp timeout	30 45 60 90 120 150 180 seconds
Park timeout	30 45 60 90 120 150 180 300 600 seconds
Page timeout	15 30 60 120 180 300 600 2700 seconds
Transfer callback timeout	3 4 5 6 12
Host delay	200 400 600 800 1000 1200 1400 1600 1800 2000 milliseconds
Link time	100 200 300 400 500 600 700 800 900 1000 milliseconds

Release Reasons

The **Release reasons** heading allows you to determine the level of system reporting you require for released ISDN calls. You can choose to have no text, a simple explanation, or a detailed explanation.

To set **Release reasons**, follow these steps:

1. Click on the keys beside **Services**, **Telephony Services**, and **General settings**.
2. Select **Release reasons**.

   The Release Reasons screen appears.
3. Table 105 lists the possible values for Release reasons.

Table 105 Release reason values

Attribute	Values	Description
None	Default value	No text will accompany a dropped call notification.
Simple	Cause code: On, Off	If the cause code is off, no text is provided. If the cause code is on, the code only is provided.
Detailed	No settings	If detailed is selected, a detailed explanation of the cause code is provided.

Note: If you select Simple text, you must turn off the Cause code. This is for diagnostics.

System Speed Dial

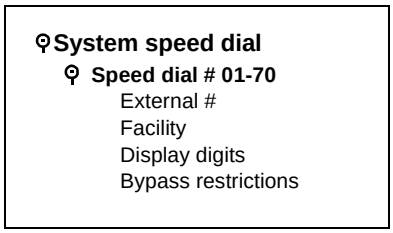
The System speed dial heading allows you to specify speed dial codes (01 - 70) and external numbers that any telephone set on the system can use.

Task:

Set up the system so users can dial frequently-called numbers with just two digits.

The following illustration shows the System speed dial programming map.

Figure 48 System speed dial headings



Adding or Changing a System Speed Dial

You can program a speed dial on your Business Communications Manager system so that anyone in your office can dial a frequently-used number using a two-digit code. Examples of system speed dials might include telephone numbers of regional sales offices within your organization or key customers that you call frequently.

To change a speed dial that already exists, follow the same steps as if you are creating a new system speed dial. The new programming overwrites the previous number and settings.

If you are creating a system speed dial for the first time, you will need to choose the type of facility for the system speed dial. For more information about programming line facilities, see “Creating a System Speed Dial” on page 267.

The system has a standard name to display, so it is not necessary for you to program one; however, if you choose not to display the telephone number, you may want to create a more descriptive name.

Creating a System Speed Dial

1. Click on the keys beside **Services**, **Telephony Services**, and **System speed dial**.
2. Click a **Speed dial number** (Speed dial # 01 to 70).
3. In the **External #** box, type the telephone number (up to 24 digits), and then press **Enter**.

   If this is a new speed dial, more fields appear after you press Enter.

4 Click a Facility value: **Use prime line**, **Use line:nnn**, **Pool code:x**, or **Use routing table**.

Note: If you assign a specific line to a system speed dial number, only telephones with an appearance of that line can use the speed dial number.

5 Click a Display digits value: **Y** (Yes) or **N** (No).

Note: If you choose not to display the digits, the name of the Speed Dial code is displayed instead of the phone number. The default is Y.

6 Click a Bypass restrictions value: **Y** (Yes) or **N** (No). The default is **N**, the Speed dial number will not bypass the line and set restrictions already programmed.

System Speed Dial Matrix

To help you organize your system speed dial information, transfer the following information to a spread sheet. The outgoing name is not supported on BRI (North America).

Table 106 System speed dial matrix

Speed dial #: (01-70)	External #	Facility	Display digits	Bypass restr'n
		Use prime line Pool code:___ Use routing tabl:___ Use Line: ___	Y N	Y N

Telco Features

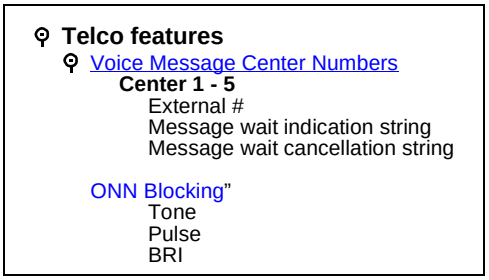
The Telco features commands allow you to define settings for voice message center numbers and outgoing name and number blocking (ONN).

Task:

- Set up voice message access and control strings
- Set up the method for blocking outgoing set identification.

Figure 49 shows a detailed view of the Telco Features navigation tree.

Figure 49 Telco features headings for voice messaging and ONN



Voice Message Center Numbers

If you subscribe to a voice message service outside your office, you can access it through your Business Communications Manager system. You can specify what voice message center you use for each external line that receives message waiting indication. This setting specifies the external telephone numbers that the Message feature dials to retrieve voice messages.

Note: If you have an MCDN link set up with a Meridian 1, for example, you would need to ensure that the number of the voice mail system is entered here.

1. Click on the keys beside **Services**, **Telephony Services**, and **Telco features.**
2. **Click on the key beside Voice message center numbers**.
3. Click the Center number you want to program. For example, **Center 1**.
   The Center 1 screen appears.
4. Table 107 on page 269 explains the settings for the Center # screen.

Table 107 Voice message center settings

Field	Values	Description
External #	<phone number>	This is the number of the remote voice message system.
Message wait indicate string	<string>	indicates that the message center has a message in the mailbox. This is a default NSI string for message waiting.

Table 107 Voice message center settings (Continued)

Field	Values	Description
Message wait cancellation string	<string>	indicates that the voice messages have been retrieved. This is a default NSI string for message waiting.

5 Repeat for each center you want to identify.

Tips: A telephone does not show that external voice messages are waiting unless you enable External voice message set. This setting is specified for each telephone under Line Assignment. You can program up to five voice message center numbers, but many systems require only one.

ONN Blocking

When you activate Outgoing name and number blocking (ONN), a user presses [Flash] 8 1 9 to block the outgoing name and number on a per-call basis. The system flags the call to the Central Office (CO) so that the name and number is not sent to the person you call.

Business Communications Manager alerts the CO by two methods. The method used depends on the type of trunk involved in placing the outgoing call.

- Analog trunks use a dialing digit sequence called aVertical Service Code (VSC). The VSC differs from region to region and must be programmed. Analog trunks with both tone and pulse dialing trunks can have separate VSCs.
- PRI trunks have only one VSC.

Configuring ONN

Follow these steps to configure an ONN setting:

1 Click on the keys beside **Services**, **Telephony Services**, and **Telco features.**

2 Click on **ONN blocking.**

3 Table 108 explains the possible choices for ONN blocking.

Table 108 ONN blocking settings

Field	Values	Description
Tone	F78(0 to 9, *, #)	For your analog trunks, enter a digit or character to determine what code the user will enter to activate this service.
Pulse	F78(0 to 9, *, #)	For your digital trunks, except BRI, enter a digit or character to determine what code the user will enter to activate this service.
BRI	F78(0 to 9, *, #)	For your BRI trunks, enter a digit or character to determine what code the user will enter to activate this service.

Telco Features Matrix

To help you organize your system speed dial information, transfer the following information to a spreadsheet. The outgoing name is not supported on BRI (North America).

Table 109 Telco features matrix

Voice Message Center numbers			
Center	External Number	Message Wait Indication String	Message Wait Cancellation String
VMsg center 1 VMsg center 2 VMsg center 3 VMsg center 4 VMsg center 5			

ONN Blocking (F78)														
Tone	<blank>	F78	0	1	2	3	4	5	6	7	8	9	*	#
Pulse	<blank>	F78	0	1	2	3	4	5	6	7	8	9	*	#
BRI	<blank>	F78	0	1	2	3	4	5	6	7	8	9	*	#

Enhanced 911 (E911) Configuration

Government rules vary about support for Enhanced 911 (E911) dialing service by Customer Premises Equipment. Legislation may require that the Customer Premises Equipment give a more precise location of the source of a 911 call than the billing address of the central office line.

Consult your service provider about the laws and regulations.

Task:

Set up emergency access number to comply with local regulations.

Use the following configuration rules when installing the Business Communications Manager system to assure compliance with local regulations:

- When equipped with PRI trunks, Business Communications Manager can deliver the Calling Line ID of a telephone dialing 911 through the Public Switched Telephone Network, if the proper programming has been implemented and PRI trunk service has been installed by the service provider. If you are using ISDN PRI, implement OLI programming and Business Name programming to add the Set ID to the CLASS information.
- By default, Restriction Filter 02 is assigned to all sets on startup. There are no restrictions applied in Restriction Filters 02-99. Restriction Filter 01 has restrictions, but 911 is an exception for this filter. For information on how to change the Restrictions, refer to "Defining Restriction Filters" on page 190.

- When using other trunk interfaces, you can assign separate line pools to groups of telephones in different areas (for example, in different buildings, floors or sections).
- Be careful when using the Set Relocation feature. You may have to reprogram the line pool access to send the right location on 911 calls.
- Configure the 911 destination code to dial out over a Normal Schedule in all applicable Service Modes, as this is the default route should any other programmed routing attempts fail. When using PRI interfaces, make sure all sets can use the PRI line pool that the Normal Schedule route uses.

911 and IP telephones

DO NOT program IP telephones with a 911 code if the set is at a remote location from the Business Communications Manager emergency location number.

Chapter 12
Configuring Portable Services

This chapter describes the programming procedures for the two types of portable handsets that can be used with the Business Communications Manager system.

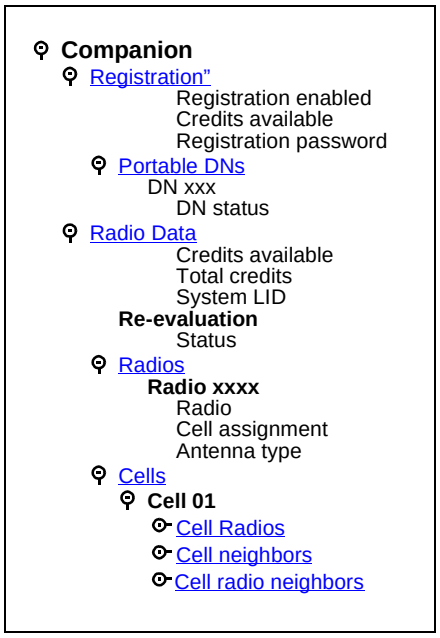
Caution: Companion Wireless systems and the DECT system have specific deployment areas and licensing requirements.
They also require a site survey prior to deployment to ensure proper distribution of the base stations around the call site.

Note: If your system has a 3/5 DS30 channel split, you can only add 32 Companion sets to your system.

Companion Wireless System

The Companion heading allows you to assign portable telephones to the system, check Base Station parameters, and enable and disable registration through programming. Figure 50 shows a detailed view of the Companion headings on the navigation tree.

Figure 50 Companion headings



Note: Companion Wireless requires a Business Communications Manager keycode to activate.

Registering Companion Handsets

The **Registration** heading under **Companion**, provides access to controls to allow you to allow or disallow handset registration. You can also enter or change a registration password, that further protects the system from unauthorized entry.

When you enable registration, the **Portable DNs** heading displays the DNs that can be used for the handsets. These DNs are the same as those found under the **Telephony Services/System DNs/ Active Companion DNs** heading.

Warning: Before you install or move wireless equipment in the United States, check that you have approval from UTAM Inc.

The United States FCC has appointed UTAM Inc. as the body responsible for coordinating and verifying the installation or relocation of unlicensed, personal wireless communication devices. To comply with UTAM Inc., the system uses keys and credits to control user capacity and to ensure system location verification. You require these software keys and credits to activate Companion services. You purchase these credits at the time you place the order.

To enable user registration or to change the password, follow these steps:

1. Select **Services/Telephony Services/Companion/Registration**.
2. Use the information in Table 110 to check registration information.

Table 110 Handset registration and password information

Attribute	Value	Description
Registration	Y, N	You must enable registration for the entire Business Communications Manager system to allow registration of individual portables. After you have registered the sets, come back and disable registration by setting this field to N.
Credits available	Read-only.	This field shows the number of credits that are available for handset registration. This number must be any positive number to allow portables to be registered. The number decrements by one with each successful registration. The number increments when a telephone is deregistered. Additional credits can be added by purchasing another keycode.
Registration password	<five digits>	Enter the digital code that needs to be identified on the handset to allow access to the system. This number can be changed, as required.
		Tips: You can choose any combination of one to six digits for the password. It is easier to remember the password if the digits spell a word. Provide this password only to selected personnel, to prevent unauthorized access to programming. The implications of such access can include the rearrangement of line assignments, which can affect the operation of the Business Communications Manager.

Warning: Password changes
Change your password to avoid incorrect registration.
To ensure accurate registration, change the Registration password before registering any portables. If there is another wireless system in radio range, and both systems have the same Registration password and Registration enabled, you can accidentally register on the other system instead of on your own.

Using Portable DNs to Show Handset Status

After you enable registration for your Business Communications Manager system, a series of extension numbers (565 to 596) are automatically available for registration. Check that an extension number is available before registering a portable telephone to it.

To view registered and available DNs:

1. Select **Services/Telephony Services/Companion/Registration/Portable DNs**.
2. Click a portable DN (for example, DN 471).

   The **DN status** box appears.

   If the extension number shows a status of Available, it is ready for registering a Companion portable telephone.

   If the extension number shows a status of Registered, a Companion portable telephone is already registered to that extension number. In this case, you can pick a different extension number, or deregister the current portable telephone. You must perform deregistration both at the portable and from Unified Manager.

Deregistering a Handset

Deregister an extension number from Unified Manager when:

- You must replace the portable due to loss or breakage.
- You want to assign the handset to a user with a different telephone number.

To deregister a portable:

1. Select **Services/Telephony Services/Companion/Registration/Portable DNs**.
2. Click a portable DN (for example, **DN 471**).

   The DN status window appears.
3. On the **Configuration** menu, click **Deregister**.

Note: This procedure does not clear the registration data in the portable. You must also deregister from the portable telephone (“on-the-air” deregistration).
For information about deregistering your portable telephone, refer to your Companion Portable Telephone User Guide.

Defining Radio Data

The Radio data heading allows you to view the number of credits available, the total number of credits and the System LID.

Radio re-evaluation automatically assigns the proper cell configuration to each radio in a Base Station. When you add or remove Base Stations, you must apply **Reevaluation** to the system.

Follow these steps to apply reevaluation to your Companion system.

1. From **Companion**, click the **Radio data** heading.

   The Radio data window appears.
2. Beside **System SLID**, enter the radio ID.
3. On the navigation menu, click on **Re-evaluation**.

   If the Re-evaluation status reads **Required**, you can carry out the re-evaluation.
4. On the **Configuration** menu click **Re-eval now** or **Schedule**.

Programming Base Station Radios

The Radios setting allows you to program base station radio settings.

Follow these steps to define the settings.

1. From **Companion**, click the key beside **Radio data**.
2. Click the key beside **Radios**.
3. Choose a radio number from the list.
4. Use the information in Table 111 to configure the radio.

Table 111 Radio settings

Attribute	Value	Description
Radio	Read-only identification number	This is the number that identifies the radio base station. A cell is the area covered by one or more radios in close proximity. As you move around your office while on a call with your portable, the call hands off from one cell to another. A call on a portable hands off from one cell to another only if Business Communications Manager assigns those cells as neighbors. Business Communications Manager automatically assigns cell neighbors and re-evaluates the cell-to-cell configuration when you add or remove base stations.
Cell assign	Unassigned Assigned	This box indicates if the cell has been activated.
Antenna type	Internal External	This is the type of antenna the radio base station is connected to.

Defining Cells

Cell programming allows you to examine settings for the cell radio, cell neighbor, and cell radio neighbor.

Follow these steps to set up cells for your Companion system.

1. Select **Services, Telephony Services**, **Companion**, **Radio data**, **Cells**.
2. Select a cell number (**Cell 01** to **Cell 32**).
3. Use the information in Table 112 to check cell information.

Table 112 Cell information

Attribute	Value	Description
Cell Radios	<five-digit number>	View the five-digit number of any radios assigned to this cell. For example, if radio 07012 is in the cell, 07012 assigned appears.
Cell neighbors	<two-digit cell number>	View the two-digit number of any cells that border a particular cell in a system. Click the cell number to see the settings: **Assigned** or **Unassigned**. For example, cell 01, Neighbour:03 and Neighbour:04 display. This means that cells 03 and 04 are assigned as cell neighbors.
Cell radio neighbors	<two-digit cell number>	View the two-digit number of any cells that border a particular cell in a system (the cell neighbors) plus any cells that border the cell neighbors. Click the cell number to see the settings: **Assigned** or **Unassigned**. For example, cell 01, Radio neighbour:03, Radio neighbour:04 display, and Radio neighbour:11. Cell 11 does not appear as a cell neighbor, therefore, it must be a neighbor of cell 03 or 04. Refer to the example under Cell neighbor.

Registering Companion Portables

To register each portable with Business Communications Manager:

- Enter the Registration password on each portable.
- Verify that the portable operates properly.

When you distribute the portables, tell the users that the portables are registered and give them the corresponding extension numbers.

Note: You cannot register a portable to more than one extension number per system. You cannot register more than one portable to one extension number.
You can register a portable to more than one system. If a portable telephone is to be used in more than one Business Communications Manager system, its owner must know which registration slot number was used to register the portable telephone with each system. Nortel Networks recommends that users register their most frequently used system in slot 1.
If a portable telephone is lost or broken, deregister it from the system before replacing it with another portable telephone.

Portable Telephone Programming

Portable telephone programming is similar to the process for programming Business Communications Manager desk telephones. Some programming settings do not affect the operation of the portable.

Table 113 shows the recommended settings for Business Communications Manager.

Table 113 Portable telephone programming

Programming level	Programming option	Setting	Notes
System DNs.../ DN XXX/Line access	Answer DNs	<set DN>	This is the number of the stationary telephone that is twinned with the handset. When the stationary telephone gets a call, the Companion mirrors the call.
System DNs.../DN XXX/Capabilities	Forward no answer	Fwd to: <DN> Fwd Delay: <no. of rings>	This stops the Companion portable from ringing when the call is forwarded to its new destination. The portable user can still answer the call, but it does not ring. The settings for Forward no answer are found under **System DNs/Active Companion DNs/DN##/ Capabilities** in the Unified Manager.
	Forward on busy	Y	
	Do not disturb on busy	N	
	Handsfree	N	
	Handsfree answerback	None	
	Pickup group	<group number>	A portable can be part of a pickup group and answers calls ringing at telephones in the same group when the user enters F*76. See “Defining Capabilities” on page 157 for more information about Group pickup.
	Paging	Y	
	Page zone	1	
	Direct dial	Set 1	A portable cannot be a Direct dial telephone. It can use the Direct dial digit.
	Hotline	None	
	Priority call	Y	Requires special configuration of hardware and programming
System DNs.../DN XXX/Restrictions/ Set Restrictions	Set lock	Y	Does not apply to portables.
	Allow last number	Y	Does not apply to portables.
	Allow saved number	Y	Does not apply to portables.
	Allow link	Y or N	This can be set to N for portables.

Companion Matrix

To help you organize your Companion handset and radio information, transfer the information in Table 114 to a spreadsheet and fill it out as you determine the features.

Table 114 Companion installation information

Registration	Registration enabled: N Y	Credits available _____	Registration Password _____
Portable DNs	DN State: Available Assigned		
Radio data: System LID:			
Reevaluation status: Required Not Required			
Radio #	Cell assignment Assigned Unassigned	Antenna type: Internal External	
Cell #	Cell Radios	Cell Neighbors	Cell Radio Neighbors

DECT Portable Systems

DECT portable systems are available in specific regions. To have DECT capability, you must have your system set to a compatible region. Refer to "Mobility Services by Region" on page 579. No keycode is required to activate this system.

The *Business Communications Manager 2.5 DECT Installation and Maintenance Guide* provides detailed installation information for the DECT media bay module and the base stations. It also includes configuration information for the DECT module, the base stations, and the cordless handsets.

The system considers the DECT cordless handset an ISDN device. Therefore, the DNs assigned to the handsets come from this range. After the routing and registration information is set up, the handsets can be configured in the same way as any other ISDN-based telephone, taking into consideration the ISDN characteristics.

DECT Matrix

To help you organize your DECT handset and base station information, transfer the information in Table 115 to a spreadsheet and fill it out as you determine the features.

Table 115 Companion installation information

Cell name	Base station name (up to eight base stations)	Base station DECT module port			
		6-0 6-1 6-2 6-3 7-0 7-1 7-2 7-3			
Portable DNs	DN State: Available Assigned	DN Type: ISDN and DECT	Twin DN	Call log passwords	

Programming for Mobile Handsets

To help you organize your mobility handset information, transfer the information in Table 116 to a spreadsheet and fill it out as you determine the features. Note that a number of the settings are not available to DECT handsets, even though it appears you can change them. These settings are indicated as not supported in the following tables.

Table 116 General and Line access settings

Sets: (max. 7 digits)	
Prime Line	Not supported.
Intercom Keys	not supported
OLI#	None #
Line assignment List three- digit line number and circle line assignment. AR = Appear&Ring A = Appear only R = Ring only blank = Unassigned	001 A R 002 A R _ _ _ A R _ _ _ A R _ _ _ A R _ _ _ A R _ _ _ A R
Call log set	not supported
Vmsg set	not supported

Answer DN	Appr & ring Ring only Appr only

Table 117 Capabilities

Sets: (max. 7 digits)	
Capabilities screen	
DND on Busy	Not supported.
Handsfree	
HF answerback	Not supported.
Pickup grp	Not supported
Page zone	1 2 3 4 5 6 None
Paging	Y N

Aux. ringer	Y N
Allow redirect	Not supported.
Redirect ring	Not supported.
Hotline	Not supported.

Call Forward	
Fwd no answer	None to:
Fwd delay	2 3 4 6 10
Fwd on busy	None to:

Intrusion	
Protect lvl	None Low Med High

Table 118 User preferences, restrictions and telco features

User preferences: Read-only	
Restrictions/Set Restrictions	
Set lock	Not supported.
Allow last number	Y N (terminal-dependent)

Allow saved number	Not supported.
Allow link	Y N (terminal-dependent)

Set restriction schedules		
Filters		
Normal	02	02,
Night	11	11,
Evening	12	12,
Lunch	13	13,
Sched 4	00	00,
Sched 5	00	00,
Sched 6	00	00,

Line/set restrictions	
Normal None	
Night None	
Evening None	
Lunch None	
Sched 4 None	
Sched 5 None	
Sched 6 None	

Telco features	
First display	automatically defined.
Auto Called ID	
Set log space	
Available log space	read-only

Chapter 13
Configuring Hunt Groups

This chapter explains how to create hunt groups using the Hunt Group headings in the Unified Manager.

Hunt groups are designed to provide a service where incoming calls appear on a targeted group of telephones (a hunt group). When you designate a hunt group, you define the group as a unique DN. This DN receives and distributes calls to telephones assigned to the group. The telephones receiving the call provide a line indication that a call has come in. How the calls are distributed can also be defined.

There can be a maximum of 30 hunt groups assigned on a Business Communications Manager.

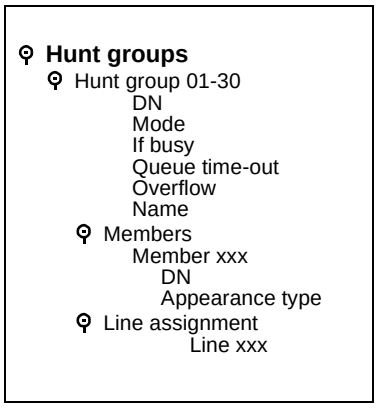
Task:

For each hunt group:

- Determine the lines for the group
- Determine how the calls will be handled and distributed.
- Determine which telephones are part of the group.

Figure 51 shows a detailed view of the Hunt groups headings on the navigation tree.

Figure 51 Hunt groups menus and fields



Some typical uses of Hunt groups are:

- a sales department answering questions on product prices or availability
- a support department answering questions concerning the operation of a product
- an emergency department answering calls for help

How Hunt Groups Work

You can use hunt groups to route calls to a support service such as a Help Line for a software company. Specialists handling Product A can be in one group, and specialists handling Product B can be in another group. Incoming calls hunt for the next available set in the group. If no set is available, the system places the call in a queue or gets routed to an overflow set.

Each Hunt Group has its own unique system DN that can be called from any set on the same system. When the hunt group DN is called, the incoming call is treated in the same fashion as calls received from lines.

A hunt group can receive a call in one of two ways:

- from one of the lines assigned to the hunt group
- from an internal system call to the hunt group DN.

Note: Do not program videophones as members of a Hunt group. Hunt groups allow one B channel connection at a time and videophones use two B channels.

Identifying a Hunt Group

When you first set up a hunt group, you need to identify how a call will be handled among the group.

1 Click the keys beside **Services**, **Telephony Services**, and **Hunt groups**.

2 Click on a Hunt group (**Hunt group 1-30**).

The Hung group ## screen appears in the right frame.

3 Table 119 describes the settings that define how a hunt group handles calls:

Table 119 Hunt group settings

Field	Values	Description
DN	Read-only	Hunt group DNs begin at 625. This value cannot be altered.
Mode	Broadcast Linear Rotary Default: Broadcast	Choose how you want the line to present to the group. **Broadcast**—simultaneously rings at each non-busy telephone in the hunt group. All telephones receiving the call also display the calling line identification from the line, if the telephone or line has been configured to offer that service. Any of the alerted telephones can access the call. Only one call can be presented to a hunt group at a time. Other calls are queued until the first call is answered. Then the next call rings on the remaining non-busy telephones. This feature allows the call load to be continuously spread across the entire member group.

Table 119 Hunt group settings (Continued)

Field	Values	Description
Mode (continued)		**Linear**—rings the first telephone in the hunt group list. If that telephone is busy, the system continues down the hunt group priority list until a non-busy telephone takes the call. In this case, all incoming calls are processed simultaneously and delivered based on the priority list. With this feature, you can program your top salesperson to be the first member of the Hunt group to receive incoming calls. **Rotary**—the call starts at the member telephone that appears on the list after the telephone that answered the last call. If that telephone is busy, the system proceeds down the priority list until a non-busy telephone is reached. As many incoming calls can be processed as there are available telephones to accept the call, each call being presented in the described round-robin fashion.
Hunt Delay	1-10 (seconds)	If Mode is either Linear or Rotary, Hunt Delay specifies how much time to delay offering a Queued call to a member telephone once that telephone becomes available. This is to provide a break period for the users between calls. The default is four seconds.
If busy	Busy tone Queue Overflow Default: busy tone	Choose how you want the system to respond if all lines appear as busy. **Busy tone**: If all lines are busy, the user receives a busy tone. **Queue**: If all lines are busy, the user is put on hold for the next available agent. **Overflow** - If all members of the Hunt Group are busy on a call from that Hunt Group, then route this call to the Hunt Group overflow DN. Overflow is only available if the overflow DN is different than the hunt group DN. Refer to the Overflow field, below.
Queue time-out	15, 30, 45, 60, 120, 180 (seconds) Default: 60	Choose the time in seconds for a call to remain in the Hunt Group. This value defines the maximum time a call remains queued, and the maximum time to offer a call before sending it to overflow if it is not answered. If the queue times out before the call connects to a member telephone, the call is terminated. If the call has been offered to a member telephone, but is not answered when the queue times out, the call is rerouted to the overflow DN.
Overflow	<any system DN> (including a Hunt Group DN) Default: hunt group DN	This setting determines where unanswered calls are routed after the Queue timeout occurs. If a call gets overflowed back to the same Hunt Group, the call goes to the bottom of the queue and is treated as a new call
Name	<an alpha-numeric string naming the Hunt Group>	Provides a unique name for the Hunt Group. The default is HGxx, where xx is the Hunt Group number 01-30.
Aux ringer	Y or N	Defines whether an auxiliary ringer (if installed) rings for incoming calls to a hunt group.
Distinct rings in use	read only	This field indicates the distinct ring patterns are currently in effect, if any, on any lines, telephones, or hunt groups on the system.

Table 119 Hunt group settings (Continued)

Field	Values	Description
Distinct ring	None Pattern 2, 3 or 4	Select a ring pattern for the hunt group. Default is none.
	Warning: If you assign a distinctive ring pattern for a telephone, and that distinctive ring pattern is currently assigned to any line as a distinctive ring, then the distinctive ring pattern for the line will be defaulted back to None. If you assign a distinctive ring pattern to a line and that distinctive ring pattern is already assigned to a telephone as the default ring pattern, then the ring pattern of those telephones will be set to pattern 1. Refer to "Distinct ring" on page 99 and "Distinct rings in use" on page 162.	

Hunt Group Members

After you determine the hunt group, you then assign members to the group.

The following limitations apply to adding member DNs to a Hunt Group:

- Any system telephone or portable can be a member of a Hunt group.
- A telephone can be in more than one Hunt group. It is considered a member in each Hunt group, which increases the total number of members in the system.
- There can be only one appearance of the same Hunt group on a set.
- Hunt group DNs cannot be members of other Hunt groups.

There are no default members to hunt groups. When a Hunt Group menu entry is first opened there will be no entries under the Members node.

Adding a Hunt Group Member

Follow these steps to add a hunt group member:

1. Click on the keys beside **Services**, **Telephony Services**, and **Hunt groups**.
2. Click the key beside the **Hunt group** (**Hunt group 1-30**).
3. Click on **Members**.
4. At the top of the navigation tree, click the **Add** button.
5. Type a set number in the **DN number** box.
6. Click the **Save** button.
7. On the navigation tree, click the member number you created or that you want to change.

   The Hunt Group ## - Member ### screen appears.

8 Choose the Appearance type to define how the call appears on the set.

- **Appr&Ring (default)**: The incoming call number appears on the display and the set rings.
- **Ring only**: The incoming call rings at the set, but no number is displayed.
- **Appr only**: The incoming call displays on the set, but the set does not ring.

Removing a Hunt Group Member

Follow these steps to remove a hunt group member:

1 Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.

2 Click the key beside the **Hunt group** (**Hunt group 1-30**).

3 Click on **Members**.

4 Click the member (for example, Member 001) to be removed.

5 Go to the top of the navigation tree and click the **Delete** button.

Removing All Members from a Hunt Group

Follow these steps to clear out the hunt group members list:

1 Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.

2 Click the key beside the **Hunt group** (**Hunt group 1-30**) from which you want to remove the members.

3 Click **Members**.

4 Go to the top of the navigation tree and click the **Delete All** button.

Moving Members of a Group

Member order within a Hunt group is important. The member order determines how a call routes through a Hunt group when the group is set to either linear or rotary mode.

To move a member within a Hunt group:

1 Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.

2 Click a **Hunt group** (Hunt group 1-30).

3 Click on the key beside **Members**.

4 Click a member from the member list (for example **Member 003**).

5 On the **Configuration** menu, click **Move**.

6 Type the new member number (001, 002, etc.) in the **Move to** box.

7 Click the **OK** button.

The system automatically reorders the list.

Programming Hunt Group Lines

Multiple lines can be assigned Hunt Group. However, a line can only exist in only one Hunt Group.

When you assign lines to hunt groups, you must ensure that there is no interruptions to the call before the hunt group DN handles the call. One of the settings that you need to check, is the designated prime set. This must be set to None. This prevents calls coming on that line from transferring to a prime set before the hunt group can handle the call.

For more information about programming line settings, refer to "Assigning Trunk/line Data" on page 97.

Assigning or Unassigning Lines to a Hunt Group

You can assign and unassign lines to hunt groups.

Assigning a Line

Follow these steps to assign a line to a hunt group:

1. Click on the keys beside **Services**, **Telephony Services**, and **Hunt groups**.
2. Click the key beside the **Hunt group** (**Hunt group 1-30**).
3. Click **Line Assignment**.
4. At the top of the navigation tree, click the **Add** button.
5. Type a line number (for example 061) in the **Line number** box.
6. Click the **Save** button.

Unassigning a Line

Follow these steps to remove a line from a hunt group:

1. Click on the keys beside **Services**, **Telephony Services**, and **Hunt groups**.
2. Click the key beside the **Hunt group** (**Hunt group 1-30**).
3. Click **Line Assignment**.
4. Click the line number (for example, **Line 061**) to be deleted.
5. At the top of the navigation tree, click the **Delete** button.

Unassigning All Lines

Follow these steps to remove all lines from a hunt group.

1 Click on the keys beside **Services**, **Telephony Services,** and **Hunt groups**.

2 Click the key beside the **Hunt group** (**Hunt group 1-30**).

3 Click **Line Assignment**.

4 At the top of the navigation tree, click the **Delete All** button.

Hunt Group Tips

Some of the things you need to note about Hunt group programming:

- calls on queue provide Ringback only (no on-hold music or tones)
- ensure the **General Settings/Timers/Transfer Callback Timer** is set correctly for hunt group configuration. Refer to "Timers" on page 265.

Feature Operation Within Hunt Groups

The operation of some features varies if the Business Communications Manager telephone is part of a hunt group. The table below shows the affected features.

Feature	Description
Call Forward All Calls	The system ignores Call Forward All Calls feature and the Hunt group call rings at the set.
Call Forward No Answer	The system ignores Call Forward No Answer and the Hunt group call continues to ring until the hunt time expires.
Call Forward on Busy	The system ignores Call Forward on Busy and the Hunt group call continues to ring until the hunt time expires.
Do not Disturb on Busy	If this feature is active, the set will not receive notification of incoming Hunt group calls.
Group Pickup	If a set is part of a Hunt group and a call pickup group, then an incoming Hunt group call can be picked up from any set that is in the call pickup group.
Transfer via Hold	The system supports transfer for Hunt group sets. However, you cannot Transfer via Hold. Once you answer a call on a Hunt group set, its appearance disappears from all other sets in the Hunt group. This means that other calls can come in on the same line.
Priority Call	You cannot make Priority calls to Hunt group DNs.
Ring Again	You cannot use Ring Again when calling a Hunt group DN.
Line Redirection	The Allow redirect attribute should be set to N for lines assigned to Hunt groups. For more information, see "Defining Capabilities" on page 157.
Page Zones	You cannot include Hunt group DNs in a Page zone.
Voice Call	Hunt groups cannot accept voice calls. Answer buttons have no appearances for voice calls, and the set does not ring.

Hunt Group Matrix

To help you organize your hunt group information, transfer the information in Table 120 to a spreadsheet and fill it out as you add Hunt groups.

Table 120 Hunt group matrix fields

Hunt Group #					
Hunt group name:	Hunt Group DN	Mode Broadcast Linear Rotary	If busy: Busy Tone Queue	Queue timeout (in seconds) 15 30 45 60 120 180	Overflow DN
Member #	DN Appr only Appr&Ring Ring only				
Line assignment					

Chapter 14
Configuring Hospitality Services

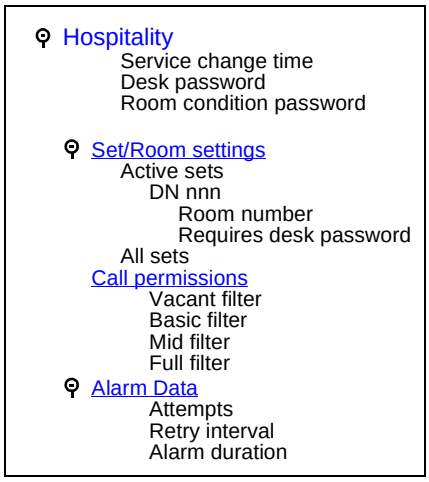
This chapter describes the Hospitality headings which allow facilities such as hotels, motels and hospitals to control telephone access to external lines, provide alarm clock services on internal telephones, and monitor room serviced status.

Task:

- Determine hospitality service change times and passwords.
- Determine room numbers for telephones.
- Determine if a telephone requires a password to access administrative-level services.
- Determine call permissions for each of the four room occupancy levels.
- Determine how the system will deal with alarms.

Figure 52 shows the Hospitality headings on the navigation tree.

Figure 52 Hospitality commands and settings



About the Hospitality Feature

In a temporary room occupancy setting, such as hotels or hospitals, guests gain improved services through immediate access to basic functions like:

- wake-up services or reminders via alarms on the room telephones
- accurate tracking of the room service requirements, such as cleaning schedules and occupancy

Hospitality Telephone Definitions

The system classifies telephones as one of three types of telephones:

Common set: This type of telephone can be found in a lobby, office, or common area. It is not associated with a room and does not have access to all of the hospitality features. These telephones are Business Communications Manager telephones or analog telephones connected to an analog terminal adapter (ATA 2), or an analog station module (ASM).

Room set: This type of telephone is assigned to a room. You can assign up to five telephones to the same room (they all share the same room number). These telephones can be any Business Communications Manager telephone or an analog telephone connected to an ATA 2 or an ASM.

Hospitality Services (HS) admin set: This type of telephone is any two-line display Business Communications Manager telephone. You can program a hospitality services telephone to require the entry of a Administrative desk password before the system grants access to hospitality administrative-level service control.

Alarm Time (AL) Feature

The Alarm time feature provides an alarm clock capability on Business Communications Manager telephones and analog telephones connected to an ATA 2 or an ASM. You can program both room telephones and common telephones to sound an audible alert at a time you request.

- You can program one Alarm time within a 24-hour period on a room or common telephone.
- You must program the alarm daily to have the alarm sound every day.
- When the alarm sounds, all telephones in a given room alert.
- When you cancel the alarm on any telephone, the alarm is cancelled on all the telephones associated with that room.
- A new Alarm time entered on a room or common telephone overwrites any previously-set alarm.
- You can determine a re-ring timer (snooze alarm) which determines when the alarm will ring again if the user paused the alarm by pressing the key (digital telephones) or by lifting the receiver (analog telephones).

Power Failures

If the Business Communications Manager system experiences a power failure, the failure can result in lost Alarm times.

When the Business Communications Manager system resumes running, and the system time resets, the missed Alarm times alert.

At all times, the Business Communications Manager system allows up to a maximum of 25 telephones that can alert at the same time.

For more information about programming this feature, see the *Business Communications Manager Telephone Features Programming Guide*.

Setting Up the Hospitality System

The Hospitality heading allows you to enter the time when occupied rooms change state from Service done to Service required. The Service change time is a primary part of the Room condition (RC) feature.

As well, you will enter desk and room passwords for the system.

1. Click the keys beside **Services** and **Telephony Services**.
2. Click on **Hospitality**.
3. Table 121 explains the possible settings for the hospitality record.

Table 121 Hospitality main settings

Field	Values	Description
Services change time	<24 hour digital time>	Identify when the occupied rooms will change from service done to service required. Format: HHMM, i.e. 1400 = 2 p.m. HH = 0 to 23; MM = 0 to 59
Desk password	<up to six digits>	Enter the password that will be required to access all the Hospitality administrative features. **Security**: We strongly recommend that you change the default password, and frequently change the desk password to prevent unauthorized entry. Default password: 4677 (HOSP)
Room condition password.	<up to six digits>	Set the password that will allow access to the Room condition feature (8 7 6). Default password: 4677 (HOSP) For more information about using 8 7 6 , see the *Business Communications Manager Feature Telephone Programming Guide*.

Identifying Room Sets

The Set/room settings allow you to assign telephones to a room. This menu also enables access control to hospitality administrative features.

1. Under the **Hospitality** heading, click on the key beside **Set/room settings**.
2. Click on the key beside **Active sets** if you are configuring a telephone that has already been set up. Click on **All sets** if you need to locate a DN for a new telephone.
3. Click a DN number.
4. Table 122 describes the two fields on the DN ### screen.

Table 122 Room settings

Field	Values	Description
Room number	<any digit from 1 to 32767>	Enter the room that contains the telephone with this DN.
Requires desk password	Y, N	If set to yes, the telephone requires a password to access administrative-level hospitality features (features 877-879). If set to no, the telephone does not require any passwords to access the features. Desk passwords are created using the main Hospitality command.

Identifying Call Permissions

The **Call Permissions** heading allows you to define dialing filters for room telephones based on the room occupancy status.

The dialing filters are standard Business Communications Manager Restriction filters (Filters 00-99). For more information, refer to “Defining Restriction Filters” on page 190. these filters are assigned to the DN of the room telephone under System DNs/Active DNs/DN## (of the room telephone)/Restrictions/Set Restrictions/Schedules.

Setting Room Restriction Filters

Follow these steps to create room restriction filters.

1. Click the keys beside **Services**, **Telephony Services**, **Hospitality**.
2. Click the **Call permissions** heading.
3. Table 123 describes the fields on the Call permissions screen. Each field can accept a two-digit code.

Table 123 Call permission settings

Field	Values	Description
Vacant filter	<two-digit code>	Enter a code that indicates which calls are allowed when a room is empty. (i.e. 911)
Basic filter	<two-digit code>	Enter a code that indicates which calls are allowed for a basic room phone. (i.e. 911, and internal calls only)
Mid filter	<two-digit code>	Enter a code that indicates which calls are allowed for a phone with mid service. (i.e. 911, internal calls, and 1-800 numbers only)
Full filter	<two-digit code>	Enter a code that indicates which calls are allowed for a phone with full service. (i.e. no restrictions)

Alarm Data

The **Alarm data** heading allows you to program how the system provides alarms to the room telephones. It also allows you to define how to be notified when an alarm expires.

Setting Alarm Parameters

1. Click the keys beside **Services**, **Telephony Services**, and **Hospitality**.
2. Click the **Alarm data** heading.
3. Table 124 describes the fields on the Alarm data screen

Table 124 Alarm data settings

Field	Values	Description
Attempts	1, 2, 3, 4, 5	Select the number of times the Alarm time feature attempts to alert the occupant before cancelling.
Retry interval	(in minutes) 2, 3, 4, 5, 6, 7, 8, 9	Select the interval between each attempt to send the alarm.
Alarm duration	(in seconds) 10, 15, 20, 25, 30, 35, 40, 45, 50	Select the period that a telephone alerts for each alarm attempt.
Time format	12 hour, 24 hour	Select the hour format to be used.

Expired Alarms

The Expired alarms setting allows you to program the system to notify a specific telephone whenever a Hospitality alarm expires by reaching the maximum number of alarm attempts, then cancelling itself without the user responding. You can also choose to allow a caller to hear a tone when an alarm expires.

Follow these steps to set expired alarms.

1. Click the keys beside **Services**, **Telephony Services**, **Hospitality**, and **Alarm data**.
2. Click **Expired alarms**.
3. Table 125 describes the fields on the Alarm data screen.

Table 125 Alarm data settings

Field	Values	Description
Notify set	None/DN: <telephone DN>	Enter a telephone DN if you want to notify a specific telephone when an alarm expires.
Use tone	Y, N	Choose whether you want the user to hear a tone when the alarm expires.

Hospitality Matrix

To help you organize your Hospitality information, transfer the following information to a spreadsheet and fill it out as you determine the hospitality features.

Table 126 Hospitality settings matrix

Hospitality	Service change time	Desk password	Room condition password	
Set/Room Settings	Room Number	Requires desk password N Y		
Call Permissions	Vacant filter: ___ Basic filter: ___ Mid filter: ___ Full filter: ___			
Alarm data	Attempts 1 2 **3** 4 5	Retry interval 2 3 4 5 6 7 8 9	Alarm duration (in seconds) 10 15 20 25 30 35 40 45 50	Time format 12 hour 24 hour
Expired alarms	Notify set: None DN:	Use tones N Y		

Chapter 15
Configuring the MSC resources

Media Services Card (MSC) resources are required for the following features:

- system functions
- voicemail and call center
- Fax mail
- IP telephony trunks
- IP clients
- Dial-on-Demand (DoD) WAN and Backup ISDN WAN connections

When you configure the MSC resources, you are configuring how Business Communications Manager shares the MSC resources between these features.

Types of MSC resources

There are several resources that you must check when you are configuring the MSC resources:

- Signaling channels
- Media channels
- DSP resources
- Voice bus paths

Signaling channels

Signaling channels are the communication channels used to send control signals to and from the MSC. You must have one signaling channel for each device you have connected and feature port you have enabled.

The number of signaling channels you have determines how many devices you can have connected and feature ports you can have enabled on your system. Signaling channels are also known as D channels.

Media channels

Media channels are the communication channels used to send voice and data information between the devices and feature ports. Media channels are required only when a device or feature is sending or receiving voice or data information. For this reason, the devices and feature ports can share media channels.

The number of media channels you have determines how many devices and feature ports can exchange voice and data information at the same time. Media channels are also known as B channels.

DSP resources

Digital Signal Processors (DSP) provide the voice processing functions on Business Communications Manager. Voice processing is required to convert voice information to and from digital format for voicemail and call center. Voice processing is also required to handle encoding and decoding of IP telephony calls. The DSPs are located on the MS-PEC cards installed in your MSC.

The number of DSP resources you have determines the number of voicemail ports, call center ports, Fax mail ports, WAN connections and IP telephony calls that can be active at the same time.

Voice bus paths

The voice bus paths are the communication channels between the DSPs on the MS-PECs and the master DSP on the MSC. One voice bus path is required for each voice processing task that is operating on the DSPs.

There are 62 voice bus paths available on Business Communications Manager.

Media gateways

Media gateways are logical connections that are a combination of DSP resources, media channels and voice bus paths that provide protocol translation between IP telephones and trunks and analog and digital telephony devices.

Rules for managing the MSC resources

The following rules are provided to assist you in configuring your MSC resources.

Signaling channel rules

Signaling channels are the MSC resource that determines how many IP telephones you can connect to your system. If you have a system that does not use IP telephones, the number of signaling channels does not affect your configuration.

- The total number signaling channels available to the MSC depends on the DS30 split you have configured. For information about how to view and change the DS30 split, refer to “Changing the DS30 Split” on page 316.
  If you have a 2/6 DS30 split, the total number of signaling channels is 64.
  If you have a 3/5 DS30 split, the total number of signaling channels is 96.
- Management functions use six signaling channels.
- Dial-on-Demand ISDN WAN uses 27 signaling channels.
  All 27 signaling channels are used, regardless of the number of WAN channels configured.
- Voicemail requires one signaling channel for each voicemail port enabled. You can enable up to 16 voicemail ports.
  Both voicemail and call center use Voicemail ports.

- IP Telephony clients require one signaling channel for each IP telephone connected to the system.
- IP Telephony trunks require one signaling channel.
  Only one signaling channel is required regardless of the number of IP Telephony trunks enabled.

Media channel rules

The media channels are used to transport voice and data signals between devices.

- Management functions use five media channels. These five channels are reserved for management functions and are always in use.
- Dial-on-Demand ISDN WAN uses 27 media channels.
  All 27 media channels are used, regardless of the number of WAN channels configured. The maximum number of WAN channels is 16.
- Voicemail and call center use one media channel for each active session.
- DECT mobility requires one media channel.
  Note: If your system also has Dial-on-Demand WAN, DECT uses one of the 27 WAN media channels, so an additional channel is not required.
- A call between an IP telephone and a digital or analog telephone or a PSTN line uses a media channel for the duration of the call.
- A call from a digital or analog telephone that uses an IP trunk uses a media channel for the duration of the call.
- A call between two IP telephones on the same Business Communications Manager uses a media channel during call setup. After the call is established, the media channel is released.
- A call on an IP telephone using an IP trunk uses a media channel during call setup. After the call is established, the media channel is released.

Since most of the devices do not use media channels all of the time, your system can have more devices than there are media channels. However, to ensure you have sufficient system resources, make sure the number of media channels you have exceeds your estimate of peak media channel usage. The section below provides an example of how to estimate your peak media channel usage.

Example of how to estimate peak media channel usage

The example below is for a fictional company named CompanyABC. The numbers used are strictly for this example. Actual numbers will vary depending on the company. When you are estimating your peak media channel usage, make sure you use numbers that reflect your business.

- CompanyABC has a Business Communications Manager system with 96 telephones. Of these telephones, 48 are digital telephones and 48 are IP telephones.
  The percentage of IP telephones is 50% (48/96). This percentage is used to estimate how many calls will be made between IP telephones and digital telephones.
- In CompanyABC, the users are typically on the telephone 15 minutes out of each hour, or 25% of the time. During peak hours, the users are on the telephone 30 minutes, or 50% of the time. Therefore, the peak usage of IP telephones is 24 (50% X 48 IP telephones).

- In CompanyABC, half of the calls are made to external destinations and half of the calls are made within the Business Communications Manager system. CompanyABC does not have IP trunks, so the calls from the IP telephones to external destinations must use PSTN lines. The peak number of IP telephone calls that use PSTN lines is 12. (50% of calls external X 24 IP telephones during peak usage).
- For internal calls, there is a 50% chance the call is made to a digital telephone. The peak number of IP telephone calls to digital telephones is 6. (50% of calls internal X 24 IP telephones peak usage X 50% number of digital telephones)
- The peak media channel usage for IP telephony is 18. (12 media channels for external calls and 6 for calls made to digital telephones.)

DSP resources rules

The number of DSP resources you have depends of the number of type of MS-PEC you have installed. For information about how to determine the MS-PECs you have, refer to "Viewing the MS-PEC configuration" on page 310.

For the purposes of calculating DSP resources, we can estimate the relative power of each configuration as follows:

- 4 MS-PEC I 24 units
- 2 MS-PEC III 42 units
- 4 MS-PEC III 84 units

The number of DSP resources you need depends on the features and type of codec you are using.

- Dial-on-Demand WAN uses 1 unit for each 64Kbit/s channel
- Voicemail and call center use 1 unit for each active session.
- Fax mail uses 6 units for each active fax channel
- IP telephone or IP trunk using G.711 codec uses 1 unit
- IP telephone or IP trunk using G.729 codec uses 3 units
- IP telephone or IP trunk using G.723 codec uses 4 units

Note: Some of the DSP resource units listed above are rounded to the nearest whole number. This is done to ease the calculation of the DSP resources you require. To calculate more accurate DSP requirements, use the DSP resource units in Table 127.

Table 127 DSP resource requirements

Feature or codec	Resource units on a MS-PEC I	Resource units on a MS-PEC III
G.729	3	2.75
G.723	4	4.2
Fax	5	6

Voice bus path

There are 62 voice bus paths available on Business Communications Manager.

- Voicemail uses one voice bus path for each active session
- Dial-on-Demand WAN uses one voice bus path for each 64Kbit/s channel that is active.
- IP telephone and IP trunks require one voice bus path when ever a media channel is required.

Media gateways

One media gateway is required for each call:

- from an IP telephone to an analog or digital telephone
- from an IP telephone using a PSTN line
- from an analog or digital telephone using an IP trunk

Determining the MSC resources you require

The following 16 questions are designed to help determine how many MSC resources you require. Based on the answers to these questions you can calculate the number of signaling channels, media channels, voice bus paths and DSP resource units you need.

Note: In the following questions, “peak periods” refers to the periods of time when there is the highest overall activity. It is necessary to consider the resource requirements for “peak periods” to determine if available voice bus paths and DSP resources meet your resource requirements at all times.

As you answer the following questions, record your answers in Table 128 on page 307.

ISDN WAN (Dial-up/Nailed-up)

1 What is the maximum required WAN bandwidth?
The range is 0 to 1 Mbit/s (16 x 64 kbit/s) in 64 kbit/s increments.

If the answer is more than zero:

- add 27 to the signaling channel count
- add 27 to the media channel count

2 What is the required WAN bandwidth during peak periods?
The range is 0 to the maximum bandwidth you entered in question 1.

For each 64 kbit/s of bandwidth:

- add 1 to the voice bus time slot count
- add 1 to the DSP resource unit count

DECT mobility

3 How many DECT media bay modules are installed?
The range is 0 to 1 media bay modules.

For each DECT media bay module:

- add 1 to the media channel count

Voice Mail and ACD

4 What is the maximum number of Voicemail ports required? Voicemail ports are used for voicemail and call center.
The range is 0 to 16 ports.

For each voicemail port:

- add 1 to the signaling channel count
- add 1 to the media channel count

5 What is the number of Voicemail ports required during peak periods?
The range is 0 to the maximum number of ports selected in question 4.

For each voicemail port

- add 1 to the voice bus path count
- add 1 to the DSP resource unit count

6 How many fax tasks will be used during peak periods?
The range is 0 to 2.

For each fax task:

- add 6 to the DSP resource unit count

Note: The fax DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to Table 127 on page 302.

IP telephones

7 What is the maximum number of IP telephones required?
The range is 0 to 90 IP telephones.

For each IP telephone:

- add 1 to the signaling channel count

8 How many IP telephones will be calling an analog or digital telephone or using a PSTN trunk during peak periods?
The range is 0 to the maximum number of IP telephones selected in question 7.

For each IP telephone:

- add 1 to the media channel count
- add 1 to the voice bus path count

9 How many IP telephones specified in question 8 will be using the G.711 codec?
The range is 0 to the maximum number of IP telephones selected in question 8.

For each IP telephone:

- add 1 to the DSP resource unit count

10 How many IP telephones specified in question 8 will be using the G.729 codec?
The range is 0 to the maximum number of IP telephones selected in question 8.

For each IP telephone:

- add 3 to the DSP resource unit count

Note: The G.729 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to Table 127 on page 302.

11 How many IP telephones specified in question 8 will be using the G.723 codec?
The range is 0 to the maximum number of IP telephones selected in question 8.

For each IP telephone:

- add 4 to the DSP resource unit count

Note: The G.723 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to Table 127 on page 302.

IP Trunks

12 What is the maximum number of IP trunks required?
The range is 0 to 60 IP trunks.

If there is more than zero IP trunks:

- add 1 to the signaling channel count

13 How many analog or digital telephones (not IP telephones) will use IP trunks during peak periods?
The range is 0 to the maximum number of IP trunks selected in question 12.

For each IP trunk:

- add 1 to the voice bus path count
- add 1 to the media channel count

14 How many IP trunks specified in question 13 will be using the G.711 codec?
The range is 0 to the maximum number of IP trunks selected in question 13.

For each IP trunk:

- add 1 to the DSP resource unit count

15 How many IP trunks specified in question 13 will be using the G.729 codec?
The range is 0 to the maximum number of IP trunks selected in question 13.

For each IP trunk:

- add 3 to the DSP resource unit count

Note: The G.729 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to Table 127 on page 302.

16 How many IP trunks specified in question 13 will be using the G.723 codec?
The range is 0 to the maximum number of IP trunks selected in question 13.

For each IP trunk:

- add 4 to the DSP resource unit count

Note: The G.723 DSP resource unit count is rounded to ease calculations. For a more accurate DSP resource unit count, refer to Table 127 on page 302.

Table 128 Required MSC resources

Question	Answer	Signaling channels	Media channels	Voice bus paths	DSP resource units
1. WAN				-	-
2. Peak WAN		-	-		
3. DECT		-		-	-
4. VM/ACD				-	-
5. Peak VM/ACD		-	-		
6. Peak FAX		-	-	-	
7. IP Sets			-	-	-
8. Peak IP Sets		-			-
9. IP Sets G711		-	-	-	
10. IP Sets G729		-	-	-	
11. IP Sets G723		-	-	-	
12. IP Trunks			-	-	-
13. Peak IP Trunks		-			-
14. IP Trunks G.711		-	-	-	
15. IP Trunks G.729		-	-	-	
16. IP Trunks G.723		-	-	-	
Totals					

Evaluation

After you have answered the questions and calculated the four totals, use the following rules to determine the required Business Communications Manager configuration.

Table 129 Evaluation of required Business Communications Manager configuration

Resource	Number required	Required configuration
Signaling channel count	58 or less	2/6 DS30 split
	59 to 90	3/5 DS30 split
	91 or more	exceeds Business Communications Manager capacity
Media channel count	58 or less	2/6 DS30 split
	59 to 90	3/5 DS30 split
	91 or more	exceeds Business Communications Manager capacity
Voice bus path count	62 or less	within Business Communications Manager capacity
	63 or more	exceeds Business Communications Manager capacity
DSP resource units	1 to 24	4 MS PEC I
	1 to 42	2 MS PEC III
	43 to 84	4 MS PEC III
	84 or more	exceeds Business Communications Manager capacity

Note: If your system requires more MSC resources than is available on your MS-PEC configuration, you can upgrade your MS-PECs. For information about how to upgrade your MS-PECs, refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide*.

Example of a Business Communications Manager configuration

Table 130 Example of required configuration

Question	Answer	Signaling channels	Media channels	Voice bus paths	DSP resource units
1. WAN	512 kbit/s (8)	27	27	-	-
2. Peak WAN	512 kbit/s (8)	-	-	8	8
3. DECT	1	-	1	-	-
4. VM/ACD	8	8	8	-	-
5. Peak VM/ACD	6	-	-	6	6
6. Peak FAX	1	-	-	-	6
7. IP Sets	24	24	-	-	-
8. Peak IP Sets	12	-	12	12	-
9. IP Sets G711	6	-	-	-	6
10. IP Sets G729	4	-	-	-	12
11. IP Sets G723	2	-	-	-	8
12. IP Trunks	32	1	-	-	-
13. Peak IP Trunks	20	-	20	20	-
14. IP Trunks G.711	12	-	-	-	12
15. IP Trunks G.729	6	-	-	-	18
16. IP Trunks G.723	2	-	-	-	8
Totals	-	60	68	46	84

Table 131 Evaluation for the example of required configuration

Resource	Number required	Recommended configuration
Signaling channel count	60	3/5 DS30 split
Media channel count	68	3/5 DS30 split
Voice bus path count	46	within Business Communications Manager capacity
DSP resource units	84	4 MS-PEC III

Configuring the MSC resources

After you have determined what MSC resource you need, you can start configuring your MSC resources.

Viewing the MSC information

You can view information about the Media Services Card (MSC) that is installed in your Business Communications Manager.

To view the MSC information:

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** heading. The Media Services Card screen appears.

2. Click the **MSC Information** tab.
The MSC Information screen appears. The information on this page is described in Figure 132.

Table 132 MSC information parameters

Attribute	Description
Description	Shows a description of the MSC
Version	Shows the hardware version of the MSC installed.
ID	Shows the serial number of the Media Services Card.

Viewing the MS-PEC configuration

There are three MS-PEC configurations available for Business Communications Manager:

- four MS-PEC I cards - This configuration provides the fewest number of DSP resources.
- two MS-PEC III cards - This configuration provides more MSC resources than the MS-PEC I configuration.
- four MS-PEC III cards - This configuration provides the maximum number of MSC resources.

To view the MS-PEC information:

1 On the navigation tree, click the **Resources** key and click the **Media Services Card** heading. The Media Services Card screen appears.

2 Click the **MS-PEC Information** tab.
The MS-PEC Information screen appears. The information in Figure 133 appears for each MS-PEC installed in the Media Services Card.

Table 133 MS-PEC information

Attribute	Description
Location	Shows the slot on the Media Services Card where the MS-PEC is installed. The Media Services Card screen shows where these slots are on the Media Services Card.
Type	Shows the type of MS-PEC installed. You can have an MS-PEC I or an MS-PEC III. Empty appears in the Type box, when there is no MS-PEC installed in the slot. **Note**: An MS-PEC III has more DSP resources than an MS-PEC I.
Hardware ID	Shows the hardware ID of the MS-PEC.
DSP 1	Shows the status of the first DSP. The DSP status can be: • **Enabled**: Indicates normal operation. • **User-Disabled**: Indicates that the DSP has been disabled. A DSP are disabled under support conditions only and requires the assistance of a Nortel Networks service representative. • **No Firmware**: Indicates the wrong type of MS-PEC is installed or a data file was deleted from Business Communications Manager. Contact your Nortel Networks service representative. • **Out of Service**: Indicates there is a hardware failure on the MS-PEC. Replace the MS-PEC with a Business Communications Manager compatible MS-PEC. • **Unsupported**: Indicates that the MS-PEC installed is for a different Nortel Networks product and is not compatible with Business Communications Manager. Replace the MS-PEC with a Business Communications Manager compatible MS-PEC. • **Unknown**: Indicates that Business Communications Manager does not recognize the type of MS-PEC installed. Replace the MS-PEC with a Business Communications Manager compatible MS-PEC.
DSP 2	Shows the status of the second DSP. The DSP status can be Enabled, User-Disabled, No Firmware, Out of Service, Unsupported, Unknown or not available (N/A). **Note**: An MS-PEC I does not have a second DSP so its DSP 2 status is N/A.

MSC Configuration

The MSC Configuration allows you to determine how the resources are assigned on your Business Communications Manager.

In some Business Communications Manager systems, the total number of features and devices that require resources exceeds the number of resources that are available. To address this issue, Business Communications Manager allows you to share the resources. By changing minimum and maximum values for each component you can fine tune this sharing.

Minimum

The minimum value is the number of resources that are always assigned to a component. You use this number to ensure a base level of service for a specific component. For example, to ensure that at least four people can be using voicemail at all times, you would enter four as a minimum value for the Voice Port component.

The resources that are not assigned using the minimum values are shared by the components. If a component needs additional resources, it can use some of the shared resources to provide service during the busy period. This method of sharing resources allows your Business Communications Manager system to adapt to the changing demands for services.

Maximum

The maximum value is the maximum number of resources that can be used by a component. You use this number to ensure a single component does not consume all of the shared resources.

The MSC Configuration you choose greatly affects the performance of your Business Communications Manager system. Make sure you consider the needs of your users, including peak usage times, when selecting the Minimum and Maximum values. Table 134 describes the advantages and disadvantages of changing these values.

Table 134 Advantages and Disadvantages of Minimum and Maximum values

	Advantage	**Disadvantage**
Increasing Minimum Value	Increases the guaranteed level of service for a component. The DSP resources you assign as a Minimum are always available to the users of this component.	Decreases the flexibility of DSP resource sharing. DSP resources that are assigned to the Minimum value are not shared with other components. If you set the Minimum level too high, other components may not be available due to a lack of available DSP resources.
Decreasing Minimum Value	More DSP resources are available to share with other components. When there is a large pool of shared DSP resources, Business Communications Manager more readily adapt to changing component use.	Lower guaranteed level of service for this component. If the Minimum value is too low, it is possible that some users will not be able to access this component when other components are in heavy use.

Table 134 Advantages and Disadvantages of Minimum and Maximum values

	Advantage	Disadvantage
Increasing Maximum Value	Allows this component to use more of the shared DSP resources during times of peak use. This allows more people to use this component at the same time.	During times of peak use, this component may consume all of the shared resources. This may cause other components to be unavailable to users.
Decreasing Maximum Value	Prevents this component from using so many of the shared DSP resources, that other components are unavailable.	Limits the number of people that can use this component even if sufficient DSP resources are available.

Viewing the MSC Configuration

To view the MSC Configuration:

1 On the navigation tree, click the **Resources** key and click the **Media Services Card** key.

2 Click the **MSC Configuration** heading.
The Configurations screen appears.

3 Click the **Current** tab.
The Current screen appears. This screen show the MSC configuration currently being used on your system.

Changing the MSC configuration

To change the MSC configuration:

1 On the navigation tree, click the **Resources** key and click the **Media Services Card** key.

2 Click the **MSC Configuration** heading.
The Configurations screen appears.

3 Set the Configurations parameters according to Figure 135.

Table 135 MSC configuration parameters

Attribute	Description
Active Configuration	Select the MSC configuration you want to use. Select **Default** to use the MSC configuration that was programmed at the factory. Select Custom1, Custom2 or Custom3 to use one of the customized MSC configuration you created. For information about how to create a custom MSC configuration, refer to "Creating a custom MSC configuration" on page 314.
Update or Reboot Required	Shows if a system reboot is required before the selected configuration is applied.
Custom 1 Name	Enter the name for the first custom MSC configuration. **Note**: You do not have to change the Custom Name to use a Custom Configuration.
Custom 2 Name	Enter the name for the second custom MSC configuration.
Custom 3 Name	Enter the name for the third custom MSC configuration.

4 Press the **Tab** key to save your changes.

Note: You must reboot the Business Communications Manager for changes to the MSC configuration to take affect.

Creating a custom MSC configuration

You can create up to three custom MSC configurations.You must create a custom MSC configuration before you can apply the configuration to the MSC.

To create custom MSC configuration:

1 On the navigation tree, click the **Resources** key and click the **Media Services Card** key.

2 Click the **MSC Configuration** heading.
The Configurations screen appears.

3 Click the Custom1 tab to change the first custom configuration.
The Custom1 screen appears.

Note: If you want to change the second custom configuration, click the **Custom2** tab. If you want to change the third custom configuration, click the **Custom3** tab.

4 Click the component you want to change (for example, IP Clients).

Table 136 MSC custom configuration parameters

Component	Description
IP Clients	IP Clients are IP telephones such as i2004 telephones and i2050 Software Phones. DSP resources are required only when the IP telephone is in use (for example, to make a call, receive a call, listen to voicemail). For information about how to configure IP clients, refer to the *Business Communications Manager IP Telephony Configuration Guide*. **Note**: The codec (G.711, G.723 or G.729) you are using for the IP Client affects how many IP clients you can use on your system.
IP Trunks	IP Trunks are communication channels that Business Communications Manager uses to send and receive IP telephony calls using the Public Data Network. You can use IP trunks to connect your Business Communications Manager system to: • another Business Communications Manager system • a Meridian 1 ITG system • a third-party H.323 end point or gateway For information about how to configure IP trunks, refer to the *Business Communications Manager IP Telephony Configuration Guide*. **Note**: The codec (G.711, G.723 or G.729) you are using for the IP Trunk affects how many IP Trunks you can use on your system.
Media Gateways	Media Gateways provide the connection between IP telephony devices (IP trunks, i2004 telephones, i2050 telephones, and H.323 terminals) and normal telephony devices (PSTN lines, T7316 telephones, T7208 telephones, T7100 telephones, etc.).

Table 136 MSC custom configuration parameters

Component	Description
Voice Ports	Voice ports are communication channels that connect users to the CallPilot Voicemail and Call Center Software. DSP resources are required only when a users connects to voicemail or call center. This includes callers hearing greetings, callers leaving messages, and users accessing their mailboxes. The minimum value for Voice Ports must be 2 or higher, unless you want to disable CallPilot VoiceMail and Call Center Software. The maximum value for Voice Ports must be 2 or higher, unless you want to disable CallPilot VoiceMail and Call Center Software. To disable CallPilot VoiceMail and Call Center Software, change the minimum and maximum values for Voice Ports to zero.
Fax	Fax ports are communication channels that connect a fax machine to a fax mailbox or a user to a Fax-on-Demand mailbox.
WAN	WAN channels are dialup ISDN WAN connections.

5 On the **Configuration** menu, click **Modify Custom 1**.
Or, right click the component you want to change and click **Modify Custom 1**.
The Custom1 screen appears.

Note: If you are configuring Custom configuration 2, click **Modify Custom 2**.
If you are configuring custom configuration 3, click **Modify Custom 3**.

6 Configure the Component parameters according to Figure 137.

Table 137 MSC component parameters

Attribute	Description
Component	Shows the name of the component you are modifying.
Minimum	Enter the number of DSP resources you want to reserve for the sole use of this component. The number you choose must be high enough to ensure proper service but low enough that it leaves DSP resources for other components. **Note**: If you set this value to zero, it is possible that this component may become inoperable if other components consume all of the DSP resources.
Maximum	Enter the maximum number of resources this component can use. Enter MAX to allow this component to use as many of the available DSP resources as is allowed by the License Limit or the Hardware Limit.
License Limit	Shows the maximum number of resources that are allowed for this component based on the software licenses purchased for this system. You can increase the License limit of a component by entering keycodes. For information about how to obtain a keycode, contact your Nortel Networks sales representative.
Hardware Limit	Shows the maximum number of resources that are allowed for this component based on the hardware installed in this system.

7 Click the **Save** button.

8 Repeat steps 6 and 7 for each component you want to change.

After you complete the changes to the custom configuration, you must change the active configuration to apply these changes to the MSC. For information on how to change the active configuration, refer to "Changing the MSC configuration" on page 313.

DTMF Configuration

The DTMF configuration sets the length of the DTMF tones generated by Business Communications Manager.

The system DTMF length may need to be adjusted because of detection errors. For example, some cellular phone tones are closer to the short DTMF millisecond range. If a company is having trouble with cellular phone connections, it may be necessary to change the DTMF length to 30 milliseconds.

To set the DTMF length:

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** key.
2. Click the **DTMF Configuration** heading.
   The DTMF Configuration screen appears.
3. In the **DTMF length** box, enter a value between 30 and 60.
   This value is the length of the tone in milliseconds.
4. Press the **Tab** key to save your settings.

Changing the DS30 Split

A DS30 channel is a group of 32 signaling channels and 32 media channels. The DS30 split determines how these DS30 channels are assigned on Business Communications Manager.

You have a choice of a 2/6 or a 3/5 split. If you choose a 2/6 split, two DS30 channels are assigned to the MSC and six are assigned to the Media Bay Modules. If you choose a 3/5 split, three DS30 channels are assigned to the MSC and five are assigned to the Media Bay Modules.

The split you choose is determined by the number of signaling channels you require for applications such as voice mail, IP trunks, IP telephones and dialup ISDN WAN connections. If you need 58 signaling channels or less for these applications, use a 2/6 DS30 split. If you need 59 signaling channels or more, use a 3/5 DS30 split.

The DS30 split is set up in the Quick Start Wizard when the system is first configured. If your signaling channel requirements change, for example you want to increase the number of IP telephones, you can change from a 2/6 setting to a 3/5 setting without losing data. All new records added after the update will reflect the new default settings. To determine what the channel requirements are, refer to "Determining the MSC resources you require" on page 303.

Warning: Ensure that the system is idle before you do this procedure. The system needs to be restarted after the setting has been changed.

Note: Ensure you have a current backup before you do this procedure.

Note: You must ensure that your system has adequate DSP resources to support an increase in voice processing traffic. To determine if you have enough DSP resources, refer to "Determining the MSC resources you require" on page 303. If you need to add MS-PEC IIIs, refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide* for installation instructions. Refer to the Business Communications Manager sales catalogue for part numbers and ordering instructions.

Warning: If you choose to change the DS30 split of your system after you have configured your system, you could risk losing data for both the core system and optional applications.
Make sure you understand the implications of the changes before you go forward with this procedure.

Warning: Changing the DS30 split from 3/5 to 2/6 will cause a Cold Start of the Business Communications Manager server. As well, ALL telephony data will be lost and restored to default values.

To change the DS30 split setting:

1. On the navigation tree, click the **Services** key and the **Telephony Services** key.
2. **Click the General settings** key and click the **DS30 Split** heading.
   The DS30 Split record appears and displays the current setting for your system.
3. If you want to change the setting, choose the other option from the list.
4. Press the **Tab** key.
   You will be prompted to restart the Business Communications Manager server.

Note: Changing the DS30 split from 2/6 to 3/5 will preserve the existing telephony data. Any new device records will have default data.

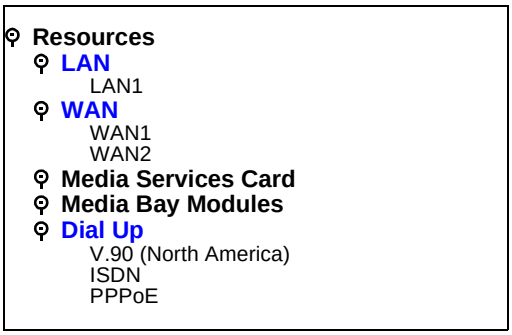
Any change in DS30 split requires a restart of the Business Communications Manager for the change to be applied.

Chapter 16\
Configuring Business Communications Manager Data Networking Resources

This chapter provides information on configuring Business Communications Manager resources.

Figure 53 shows the programming map for Business Communications Manager telephony and networking resources.

Figure 53 Hospitality commands and settings



Note: The resources listed on this table may not correspond exactly at the resources available on your Business Communications Manager system.

Viewing Business Communications Manager resources

Unified Manager lets you view and configure Business Communications Manager networking resources including LAN, WAN, and dial up resources such as ISDN or V.90 modem (North America). To view the networking resources your Business Communications Manager system supports:

1 On the navigation tree, click the **Resources** heading.
The available Business Communications Manager resources appear in a table format.

Table 138 Business Communications Manager resources

Attribute	Description
Name	Provides a list of available resources.
Status	Shows the operating status of each resource.
Version	Shows the software version of each resource.
Description	Provides a description of the interface card for each resource.

LAN

Business Communications Manager is equipped with an Ethernet/802.3 network interface card which supports the IEEE 802.3 Ethernet frame format. The Ethernet connection uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to manage the access to the physical media.

The Business Communications Manager Ethernet interface card supports the following features:

- 100 BASE T with RJ-45 connector
- 10 / 100 Auto Sense
- full duplex
- fast LAN-to-LAN routing (when using more than one LAN card)
- LAN traffic smoothing
- multiple IP addresses

Viewing the LAN resources

Unified Manager shows all available LAN resources. If your Business Communications Manager server is equipped with two LAN interface cards, Unified Manager displays all available LAN resources and names each one (LAN1, LAN2).

To view the available LAN resources:

1. On the navigation tree, click the **Resources** key and click the **LAN** heading.
   The LAN Parameters screen appears.
2. Click the Resources tab.
   The Resources screen appears.

Configuring LAN resources

Setting LAN global parameters

To set the LAN global parameters:

1. On the navigation tree, click the **Resources** key and click the **LAN** heading.
   The Lan Parameters screen appears.
2. Set your global LAN parameters according to Figure 139.

Table 139 LAN global parameters

Attribute	Description
Fast Routing (Between LANs)	Allows you to enable or disable fast routing to improve LAN-to-LAN routing performance. This feature is for a Business Communications Manager system equipped with two LAN cards. At the same link speed, a smaller packet size means more packets to forward. Use a lower traffic threshold. Permitted values: **Enabled** or **Disabled** Default: **Disabled** **Note**: Do not use Fast Routing on systems that use NAT, IP Firewall Filters, IPSec tunnels, or Quality of Service (QoS). Fast Routing bypasses these features and will cause the packets to be routed incorrectly.
Decrement TTL	When Fast Routing is enabled, Decrement TTL lets you decrement the time-to-live (TTL) value in the IP header of packets as they travel from LAN to LAN. Decrement TTL lets you increase processing time for each fast-routed IP packet, which reduces CPU cycles. This feature is used when other routers or special applications on the network connect to the LAN interfaces. Permitted Values: **Enabled** or **Disabled** Default: **Disabled**
Traffic Smoothing (In Mbps)	Lets you set the rate, in Mbps, at which the LAN driver receives packets from the LAN interface. The main purpose of this feature is to limit the number of host CPU cycles spent on LAN-to-WAN packet forwarding. Normally, LAN drivers operate at link speed, which implies that the driver forwards packets as fast as possible until there is no packet in the receiving buffer. Permitted values: **5**, **10**, **15**, **20**, **25**, **30**, **35**, **40**, **45**, **50, Disabled** Default: **40**

Table 140 Guidelines to configure LAN to LAN traffic smoothing

	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1500 bytes
Fast Routing enabled	Not needed	Not needed	Not needed	Not needed	Not needed	Not needed
Fast Routing disabled or LAN-to-WAN routing	20 mbps	30 mbps	50 mbps	50 mbps	Not needed	Not needed

Note:

The settings in the table above ensure data routing uses a maximum of 60 to 70 percent CPU cycles (Pentium III 700MHz processor).

If the LAN to WAN link speed is 10 mbps, selecting higher traffic smoothing parameters has no impact on packet forwarding, which the system still performs at a link speed of 10 mbps.

Configuring a LAN interface

To configure a LAN interface:

1 On the navigation tree, click the **Resources** key and click the **LAN** key.
The available LAN interfaces appear.

2 Click the LAN interface you want to configure (for example, **LAN1)**.
The LAN Summary screen appears.

3 Configure the LAN attributes according to Figure 141.

Table 141 LAN attributes

Attribute	Description
IP Address	Enter the IP address of the LAN interface in the following format: 255.255.255.255. If you do not know your LAN interface IP address, contact your network administrator or your Internet service provider.
SubNet Mask	Enter the subnet mask of the LAN interface in the following format: 255.255.255.255. If you do not know your subnet mask address, contact your network administrator or your Internet service provider.
Physical Address	Shows the physical address (MAC address) of the LAN interface. This is a read only attribute.
Description	Provides a description of the network interface card supporting the LAN connection. This is a read only attribute.
Version	Shows the version of the LAN interface card. This is a read only attribute.
Speed	Shows the speed of the connection to the LAN interface. This is a read only attribute.
Connection Type	Select a type of connection to the LAN interface. The following values are supported and are interpreted as follows: **Auto Sense**: The LAN interface uses the auto negotiation protocol to choose the maximum possible speed of the connection. Depending on the connected device, the LAN can choose 100 MB or 10MB and full-duplex or half-duplex. **10 MB Half**: The speed is set to 10 Mbit/s and the mode is set to half-duplex. **10 MB Full**: The speed is set to 10 Mbit/s and the mode is set to full-duplex. **10 MB Auto**: The speed is set to 10 Mbit/s and the mode (half-duplex or full-duplex) is automatically selected by the interface, using the auto negotiation protocol. The **10MB Auto** connection type limits the maximum traffic coming into Business Communications Manager to 10 Mbit/s, and enables the auto negotiation feature for easier interconnection. Limit the incoming traffic if you notice that the bursty traffic from the connected LAN is degrading the quality of voice calls carried through VoIP over the WAN. Though the LAN traffic gets lower priority in Business Communications Manager, high incoming LAN traffic to the Business Communications Manager server can result in service interruptions in the system These interruptions may degrade the quality of voice calls carried as VoIP. **100 MB Half**: The speed is set to 100 Mbit/s and the mode is set to half-duplex. **100 MB Full**: The speed is set to 100 Mbit/s and the mode is set to full-duplex. Default value: **Auto Sense** **Important**: If you have an i2004 IP telephone on your network, you must set the Connection Type to **Auto Sense**.

Table 141 LAN attributes (Continued)

Attribute	Description
Status	Shows the current status of the LAN connection. The possible states are: **Up**: The LAN card is operational. **Down**: The LAN card is not operational. This is a read only attribute.
Primary Wins Address	Enter the IP address of the Primary WINS server in the following format: 255.255.255.255.

Note: Consult your network administrator for the appropriate configuration information before changing the settings.

When you change these parameters, you must reboot the Business Communications Manager system.

Note: Setting the LAN connection speed to 100 Mbit/s does not reduce performance. However, the CPU is more efficient if you limit your incoming traffic to 10 Mbit/s. To increase your CPU performance, set the connected external LAN hub or switch to **10 Mbit/s** or to **Auto Sense**.

Note: If you enable LAN Traffic Smoothing, the connection type defaults to Auto Sense. Therefore, you do not need to set the connection speed on the external LAN hub or switch.

Configuring multiple IP addresses for the LAN interface

To add an additional IP address

1. On the navigation tree, click the **Resources** key and click the **LAN** key.
2. Click the heading of the LAN resource you want to modify (for example, LAN1).
   The LAN Summary screen appears.
3. Click the **Additional IP Address** tab.
   The Additional IP Address screen appears.
4. On the **Configuration** menu, click **Add Additional IPAddress**.
   The Additional IP Address screen appears.

5 Configure the Additional IP Address parameters according to Figure 142.

Table 142 Additional LAN IP address parameters

Attribute	Description
Range (A#)	Enter the Additional IP Address identifier. The Range number uniquely identifies an Additional IP Address. The value for this setting must follow certain conventions. You must type the prefix 'A' followed by a unique number identifying the Additional IP Address. For example, 'A2' is a valid name. If you specify an existing Range number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Range number does not have any significance, other than uniquely identifying an Additional IP Address.
IP Address	Enter the Additional IP address of the LAN interface in the following format: 255.255.255.255.
SubNet Mask	Enter the subnet mask of the LAN interface in the following format: 255.255.255.255. If you do not know your subnet mask address, contact your system administrator or your Internet service provider.

6 Click the **Save** button.

To modify an Additional IP Address

1 On the navigation tree, click the **Resources** key and click the **LAN** key.

2 Click the heading of the LAN resource you want to modify (for example, LAN1).
The LAN Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to modify.

5 On the **Configuration** menu, click **Modify Additional IPAddress**.
The Additional IP Address screen appears.

6 Change the Additional IP Address parameters.

7 Click the **Save** button.

To delete an Additional IP Address

1 On the navigation tree, click the **Resources** key and click the **LAN** key.

2 Click the heading of the LAN resource you want to modify (for example, LAN1).
The LAN Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to delete.

5 On the **Configuration** menu, click **Delete Additional IPAddress**.
A confirmation dialog box appears.

6 Click the **Yes** button.

Viewing LAN performance

1 On the navigation tree, click the **Resources** key and click the **LAN** key.

2 Click the heading of the LAN resource you want to view (for example, LAN1).
The LAN Summary screen appears.

1 On the **Performance** menu, click **LAN Graph**.
The LAN Graph: Statistic Chart screen appears.

2 On the **Performance** menu, click **LAN Table**.
The LAN Table: Statistic Table screen is appears.

WAN

A WAN (wide area network) is a geographically dispersed data communication network. The term WAN distinguishes a broader data communication structure from a local area network (LAN). A WAN can be privately owned or rented, but is usually part of public (shared user) networks.

Business Communications Manager can be equipped with aWAN interface card with two serial synchronous ports (Europe), or a WAN interface card with one T1 port (with integrated CSU) and one serial synchronous port (North America). Both ports on the WAN interface card (WAN1 and WAN2) can be active at the same time. The serial synchronous port supports the following:

- North America: V.35
- Europe: V.35 (Upper Sync Port) and X.21 (Lower Sync Port)
- maximum line speed: 8 Mbit/sec.

Business Communications Manager provides primary and backup WAN links through dial-up connections using a V.90 modem (North America) or ISDN BRI/PRI. For information on V.90 modem or ISDN connections, see “Dial Up” on page 338. Net Link Manager provides continuous WAN connection status monitoring. For information on Net Link Manager, see “Net Link Manager” on page 412.

Permanent WAN Connection

The permanent WAN connection is normally a dedicated network adapter. The permanent link supports frame relay or Point-to-Point protocol (PPP) at the link layer. The link protocol you use depends on the existing network or on the service you buy from your Internet service provider. The two ports provided by the WAN interface card can be independently configured to run frame relay or PPP.

Frame Relay

Business Communications Manager supports frame relay in group mode. For each physical port (serial sync or T1 port), there is one IP address for all PVCs (permanent virtual circuits). The available Data Link Control interface numbers are 0-1023. Of the 1023 PVCs, 16 are reserved. The maximum number of PVC’s allowed is 1008.

Point-to-Point-Protocol (PPP)

Point-to-Point Protocol (PPP) is a full-duplex transmission protocol for communication between two computers using a serial interface. A typical PPP connection is a personal computer connected by telephone line to a server. For example, your Internet service provider (ISP) provides you with a PPP connection so that the ISP server can respond to your requests, pass them on to the Internet, and return your requested Internet responses to you.

Multi-link Point-to-Point Protocol (MLPPP)

MLPPP is used to connect multiple B-channels together when using PRI or BRI ISDN as the WAN interface. This allows Business Communications Manager to connect B-channels independently of each other so that the ISDN connection can be used for both voice and data.

WAN Data Compression

Business Communications Manager provides a WAN Data Compression feature. You can use data compression on a permanent WAN connection and on a backupWAN connection.WAN Data Compression is enabled by default. You can enable or disable WAN Data Compression from the "Setting WAN Frame Relay Parameters" on page 331 screen or from the "WAN PPP Parameters" on page 335 screen, depending on your system configuration.

On a permanent WAN connection, Business Communications Manager supports the following data compression protocols:

- Frame Relay Forum standard FRF.9 data compression protocol withSTAC compression algorithm
- PPP Compression Control Protocol (RFC 1962) with STAC compression algorithm

On dial-up WAN connections, Business Communications Manager supports the following data compression protocol:

- Microsoft Point-to-Point Compression (MPPC), RFC 2118

Viewing WAN Resources

To view available WAN resources:

1. On the navigation tree, click the **Resources** key and click the **WAN** heading.
   The Resources screen appears.

Setting global WAN parameters

If PPP is the link protocol for a WAN interface (WAN1 or WAN2), you can restrict access to the network using the PPP Password List. Business Communications Manager uses the information on this list to verify and confirm the identity of the user. Only those users whose names appear on the PPP Password List can access the network. The PPP Password List configuration lets you add, modify or delete an item on the list.

To create a PPP Password List

1. On the navigation tree, click the **Resources** key and click the **WAN** heading.
   The Resources screen appears.
2. Click the PPP Password List tab.
   The PPP Password List screen appears.

3 On the **Configuration** menu, click **Add PPP User&Password**.
The PPP Password List dialog box appears.

4 Configure the PPP password parameters according to Figure 143.

Table 143 PPP password parameters

Attribute	Description
(P#)	Enter the PPP Password identifier. The PPP Password number uniquely identifies an PPP User and Password. The value for this setting must follow certain conventions. You must type the prefix 'P' followed by a unique number identifying the PPP User and Password. For example, 'P2' is a valid name. If you specify an existing PPP Password number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The PPP Password number does not have any significance, other than uniquely identifying a PPP User and Password.
PPP User Name	Enter the user name associated with the computer you want Business Communications Manager to identify as a valid network user. You must overwrite the default user name User with the user name you want to add to the list.
PPP Password	Enter the password you want to assign to the user defined in the PPP User Name box. The password can contain a combination of lowercase and uppercase letters and numbers.

5 Click the **Save** button.

To modify an existing item on the PPP Password List

1 On the navigation tree, click the **Resources** key and click the **WAN** heading.
The Resources screen appears.

2 Click the PPP Password List tab.
The PPP Password List screen appears.

3 Click the PPP Password you want to modify.

4 On the **Configuration** menu, click **Modify PPP User&Password**.
The PPP Password List dialog box appears.

5 Change the PPP password parameters.

6 Click the **Save** button.

To delete an item from the PPP Password List

1 On the navigation tree, click the **Resources** key and click the **WAN** heading.
The Resources screen appears.

2 Click the PPP Password List tab.
The PPP Password List screen appears.

3 Click the PPP Password you want to delete.

4 On the **Configuration** menu, click **Delete PPP User&Password**.
A confirmation dialog box appears.

5 Click the **Yes** button.

Configuring WAN Summary Parameters

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Configure the WAN Summary settings according to Figure 144.

Table 144 WAN summary parameters

Attribute	Description
IP Address	Enter the IP address of the WAN interface. The WAN IP address must be in the following format: 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
SubNet Mask	Enter the subnet mask address of the WAN. The subnet mask IP address must be in the following format: 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
Physical Address	Shows the physical address of the WAN interface.
Description	Provides a description of the network interface card that supports the WAN connection.
Port	Shows the port type of the WAN interface.
Version	Shows the version of the WAN interface.
Maximum Link Speed	Shows the operational speed of the WAN interface.
Status	Shows the current resource status of the WAN interface. The possible states are: **Up**: The WAN card is operational. **Down**: The WAN card is not operational.
Link Protocol	Lets you select a WAN link protocol. The options are **Frame Relay** or **PPP** protocol. The default is **Frame Relay**. If you change the link protocol, the configuration screen changes to include fields corresponding to the link protocol you choose. To ensure proper operation, always refresh the page by clicking **View** and then **Refresh**. The link protocol you choose depends on the existing network or the service you buy from your Internet services provider.
Compression	Lets you enable or disable data compression for this interface. The possible values are: **Enabled**, **Disabled** The default is **Disabled**.
Frame Size	Lets you specify the maximum frame size for the layer-2 packet carried on this port. The default is **1500**. **Note**: The Frame Size you enter must be consistent with the maximum frame size that you use use on your network.

4. Press the **TAB** key to save your settings.

Note: Unified Manager refreshes the link protocol screen according to the chosen protocol. Your choice of protocol depends on the existing network or the service you buy from your Internet service provider. Frame relay is the default link protocol. If you change the link protocol the following message appears “Reminder! Previous setting requires rebooting the system to take effect. Please reboot the system...” Click **OK**.

Caution: Reboot the system
You must remember to reboot your system for the changes you made to the link protocol to take effect. You can continue Resources configuration and reboot the system at a convenient time.

Setting WAN Line Parameters

The WAN Line Parameters screen is displayed when configuring a T1 port (North America only). Business Communications Manager supports T1 and fractional T1. Refer to the **Port** box on the WAN Summary Parameters screen to see which type of port your are configuring.

Note: The WAN Line Parameters screen is only available on the WAN1 interface.

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** heading.
   The WAN Summary screen appears.
3. Click the **WAN Line Parameters** tab.
   The WAN Line Parameters screen appears.
4. Configure the WAN Line Parameters according to Figure 145.

Table 145 WAN line parameters

Attribute	Description
Channel Rate	Lets you set the data transmission rate for each of the DS0 channels in the T1 line. Possible values are **64K** or **56K**. The default value is **64K**.
Clock Source	Lets you set an internal or external T1 clock source. Possible values are **External** or **Internal**. The default value is **External**.
Frame Type	Lets you set the type of framing the T1 line supports. Possible values are **ESF** or **SF(D4)**. The default value is **ESF**. Use the setting your T1 service provider recommends.

Table 145 WAN line parameters (Continued)

Attribute	Description
Line Coding	Lets you set the type of encoding used in the T1 line. Possible values are **B8ZS** or **AMI**. Use the setting your T1 service provider recommends.
Line Polarity	Lets you set **Normal** or **Inverted** line polarity in the T1 line. Select **Inverted** only if Line Coding is set to **AMI**.
Pulse Density	Lets you control whether the DSU/CSU maintains the minimum level of 1s on the line for AMI encoding. Possible values are **Enabled** or **Disabled**. Default value is **Disabled**.
Channel List	Lets you create a list of T1 channels used when using fractional T1. You can list each channel number or provide a range of numbers separated by a comma or hyphen. The channel list can contain a mix of ranges and individual channel numbers. For example, a valid channel list format is 3,5,6,10-15,18,20-23. To use all the available T1 channels, type **All.** Your T1 service provider can give you this information. Default value is **All**.

Note: Always use the same frame type and line coding method as your service provider.

5 Press the **Tab** key to save the settings.

Setting WAN Sync Parameters

The WAN Sync Parameters screen is only available on the WAN2 interface.

1 On the navigation tree, click the **Resources** key and click the **WAN** Key.

2 Click the **WAN2** heading.
The WAN Summary screen appears.

3 Click the **WAN Sync Parameters** tab.
The WAN Sync Parameters screen appears.

4 Click the **Clock Mode** list box and select the appropriate clock mode. You can select **DTE**, **DCE** or **Symmetrical**.

5 Press the **Tab** key to save the settings.

Setting WAN Frame Relay Parameters

If you chose frame relay as your link protocol, set theWAN Frame Relay Parameters.

1 On the navigation tree, click the **Resources** key and click the **WAN** Key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **WAN Frame Relay Parameters** tab.
The WAN Frame Relay Parameters screen appears.

4 Configure the WAN Frame Relay Parameters according to Figure 146.

Table 146 WAN frame relay parameters

Attribute	Description
LMI Type	Select the type of local management protocol used on this link. The link management type must be the same as the one used by the frame relay service provider. The available options are **Original LMI, ANSI T1.617 Annex D** or **ITU-T Q.933 Annex A**. The default setting is **Original LMI**. Note: The most commonly used setting for this parameter is **ANSI T1.617 Annex D**.
Polling Interval	Enter an interval, in seconds, between LMI status inquiry messages. The polling interval must be the same as the one used by the frame relay service provider's switch. Possible values are between **5** and **30** seconds. The default setting is **10**.
Full Enquiry Interval	Enter the maximum number of LMI Status Enquiry messages sent before sending a Full Status Enquiry request. This value must match the corresponding value set in the frame relay service provider's switch. Possible values are between **1** and **255** (in seconds). The default setting is **6**.
Error Threshold	Enter the maximum number of consecutive failures permitted in LMI Status Enquiry before dropping the link. It is also the number of successful consecutive LMI Status Enquiry messages that must be received before marking a link as operational. If you have a backup WAN connection and Net Link Manager configured, the backup connection is started and traffic is routed to the backup when this link is dropped. Also, the backup WAN connection is dropped and traffic is routed to this link when the link is operational. For information about Net Link Manager, refer to "Net Link Manager" on page 412. Possible values are between **0** and **65000**. The default value is **3**.
Monitored Events	Enter the number of events sampled for making decisions about the error threshold. This value must be set to a higher number than the value set in the **Error Threshold** box. Possible values are a number between **0** and **65000**. The default value is **4**.
DS Code	Enter the Differentiated Services code (DSCode) recognized by the frame relay driver for traffic prioritization. This value is a mask value. When an IP packet is sent, the frame relay driver checks if the packet's DSCode field (in the IP header) has any of the bits defined in the **DS Code** and sets the Discard Eligible (DE) bits to No.
Available PVCs	Shows the PVCs (Permanent Virtual Circuits) available for this WAN interface.

Table 146 WAN frame relay parameters

Attribute	Description
Compression Enabled PVCs	Enter a list of PVCs on which data compression is enabled. The value can be a comma-separated list of DLCI (Data Link Connection Identifier) numbers. You can define a range of DLCIs by inserting a hyphen between the lower and the upper boundaries. A list can contain individual DLCI numbers and DLCI ranges. If data compression is enabled, compression and decompression operations are performed on the data going to and coming from the PVCs on this list.
Access Rate	Enter the maximum access rate on the interface running frame relay in kbps. The frame relay congestion control engine uses this value to limit or shape traffic. The **Access Rate** value is determined using the T1 channels available for data communication on the port attached to this interface and their data rates.

5 Press the **Tab** key to save the settings.

PVC Congestion Control

If frame relay is your link protocol, you must configure PVC Congestion Control. If PPP is your link protocol, there are no PVC Congestion Control settings to configure.

To add PVC congestion control:

1 On the navigation tree, click the **Resources** key and click the **WAN** Key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **PVC Congestion Control** tab.
The PVC Congestion Control screen appears.

4 On the **Configuration** menu, click **Add PVC Congestion Control**.

5 Configure the WAN PVC Congestion Control parameters according to Figure 147.

Table 147 WAN PVC congestion control parameters

Column	Description
Entry (CC#)	Define each congestion control entry on the interface. A congestion control entry must use the following format: CC#, where the prefix 'CC' is followed by a number. For example, 'CC2' is a valid congestion control entry. Each entry must use a different number.You must use consecutive numbers when entering congestion control entries. If you do not use consecutive numbers, the system adjusts them to be consecutive. If you add an existing entry, the existing entry is modified with new values. When you modify an entry, the name cannot be changed.
DLCI	Enter the data link connection identifier (DLCI) number of the PVC on which to perform congestion control. A DLCI must be configured for congestion control to be performed. Business Communications Manager uses one-second intervals to measure this parameter.

Table 147 WAN PVC congestion control parameters

Column	Description
CIR	Enter the committed information rate in kbits. The CIR is the rate the carrier guarantees that the router transmits at over a predetermined time interval when congestion is not present. Contact your service provider for the correct setting. Business Communications Manager uses one-second intervals to measure this parameter.
Committed Burst BC	Lets you define the number of bits, in kbits, the router transmits over a specified time interval if congestion is present. As a rule this value is set for 1/4 the value of the CIR. Business Communications Manager uses one-second intervals to measure this parameter.
Excess Burst BE	Combined with the committed burst rate, lets you set, in kbits, the maximum number of bits the router transmits over a predetermined time interval if there is no congestion. The combined value of committed burst and excess burst must be less than or equal to the line speed.

6 Click the **Save** button.

To modify a PVC congestion control entry:

1 On the navigation tree, click the **Resources** key and click the **WAN** Key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **PVC Congestion Control** tab.
The PVC Congestion Control screen appears.

4 Click the entry you want to modify in the PVC Congestion Control table

5 On the **Configuration** menu, click **Modify PVC Congestion Control**.
The PVC Congestion Control dialog box appears.

6 Change the PVC congestion control parameters.

7 Click the **Save** button.

To delete a PVC congestion control entry:

1 On the navigation tree, click the **Resources** key and click the **WAN** Key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **PVC Congestion Control** tab.
The PVC Congestion Control screen appears.

4 Click the entry you want to delete in the PVC Congestion Control table.

5 On the **Configuration** menu, click **Delete PVC Congestion Control**.
A message prompts you to confirm the deletion.

6 Click the **Yes** button.

WAN PPP Parameters

If you chose PPP as your link protocol, set theWAN PPP Parameters screen.

1. On the navigation tree, click the **Resources** key and click the **WAN** Key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **WAN PPP Parameters** tab.
   The WAN PPP Parameters screen appears.
4. Configure the WAN PPP Parameters according to Figure 148.

Table 148 WAN PPP parameters

Attribute	Description
LCP Keep Alive Interval	Enter the interval, in seconds, to send a keep alive signal when there is no regular traffic on the PPP link. The default value is **10**.
LQR Interval	Enter the interval, in 1/100 second, to perform link quality monitoring.
Authentication Mode	Specify if a remote user can use PAP or CHAP or if the remote user is restricted to use CHAP only.
Outgoing Authentication	Select the type of authentication information that is sent to the far end of the PPP connection. You can select **ComputerName-Password** or **UserName-Password**. Selecting **ComputerName-Password** will send the name of the Business Communications Manager and the password you enter below. Selecting **UserName-Password** will send the user name and password you enter below.
User Name	Enter the user name that is used for authentication by the far end of the PPP connection.
Password	Enter the password that is used for authentication by the far end of the PPP connection.

5. Press the **Tab** key to save your settings.

Configuring multiple IP addresses for the WAN interface

To add an additional IP address

1. On the navigation tree, click the **Resources** key and click the **WAN** key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. Click the **Additional IP Address** tab.
   The Additional IP Address screen appears.
4. On the **Configuration** menu, click **Add Additional IPAddress**.
   The Additional IP Address screen appears.

5 Configure the Additional IP Address parameters according to Figure 149.

Table 149 Additional WAN IP addresses

Attribute	Description
Range (A#)	Enter the Additional IP Address identifier. The Range number uniquely identifies an Additional IP Address. The value for this setting must follow certain conventions. You must type the prefix 'A' followed by a unique number identifying the Additional IP Address. For example, 'A2' is a valid name. If you specify an existing Range number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Range number does not have any significance, other than uniquely identifying an Additional IP Address.
IP Address	Enter the Additional IP address of the WAN interface in the following format: 255.255.255.255.
SubNet Mask	Enter the subnet mask of the WAN interface in the following format: 255.255.255.255. If you do not know your subnet mask address, contact your system administrator or your Internet service provider.

6 Click the **Save** button.

To modify an Additional IP Address

1 On the navigation tree, click the **Resources** key and click the **WAN** key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to modify.

5 On the **Configuration** menu, click **Modify Additional IPAddress**.
The Additional IP Address screen appears.

6 Change the Additional IP Address parameters.

7 Click the **Save** button.

To delete an Additional IP Address

1 On the navigation tree, click the **Resources** key and click the **WAN** key.

2 Click the **WAN1** or **WAN2** heading.
The WAN Summary screen appears.

3 Click the **Additional IP Address** tab.
The Additional IP Address screen appears.

4 Click the Additional IP Address you want to delete.

5 On the **Configuration** menu, click **Delete Additional IPAddress**.
A confirmation dialog box appears.

6 Click the **Yes** button.

WAN performance

To access the WAN Primary Link performance graphs and tables for a particularWAN interface:

1. On the navigation tree, click the **Resources** key and click the **WAN** key.
2. Click the **WAN1** or **WAN2** heading.
   The WAN Summary screen appears.
3. On the **Performance** menu, click **WAN Graph**.
   The WAN Graph: Statistic Chart appears.
4. On the **Performance** menu, click **WAN Table**.
   The WAN Table: Statistic Table appears.

Dial Up

Business Communications Manager lets you create and use dial up connections for Remote Access Service (RAS) or dial-on-demand network access. RAS lets you access Business Communications Manager remotely by making an IP connection using PPPoE, an ISDN BRI/PRI line or the V.90 modem (North America only). After you connect to the Business Communications Manager system, you can access all IP-based system management operations.

Business Communications Manager also supports dial-on-demand for primary and backupWAN connections. Primary and backupWAN connections can use an ISDN BRI/PRI line or aV.90 modem (North America).

Configuring the Dial Up Global parameters

1 On the navigation tree, click the **Resources** key and click the **Dial Up** heading.
The RAS Server TCP/IP Configuration screen appears.

2 Configure the RAS Server TCP/IP settings according to Figure 150.

Table 150 RAS server TCP/IP parameters

Attribute	Description
Allow Network Access	Select whether to allow dial up access to the entire network (**Yes**) or to restrict access to Business Communications Manager only (**No**). When using dial up for dial-on-demand WAN connection (as a primary or back up WAN connection), set **Allow Network Access** to **Yes**. When using dial up for remote system management purposes only, set **Allow Network Access** to **No**.
Static IP Address Pool	Enter the IP address Business Communications Manager assigns when a remote site dials into the Business Communications Manager system. The default value is **10.10.10.5**.
Address Mask	Enter the IP address mask corresponding to the IP address range. The IP addresses from the static address pool then reserved for assignment to remote sites. The default value is **255.255.255.240**.

3 Press the **TAB** key to save your settings.

V.90 modem (North America) Dial Up

Business Communications Manager is equipped with an internal V.90 modem that connects to your phone line with a RJ-11 connector. The V.90 modem has the following features:

- V.90 56 kbps ITU standard
- V.34 33.6 kbps ITU standard
- V.42/MNP 2-4 error control
- V.42 bis/MNP 5 data compression
- compatible with ITU and Bell Standards from 56 kbps down to 1200 bps

Note: The modem is capable of receiving at a maximum speed of 56 kbps and transmitting at a maximum speed of 31.2 kbps. Because of FCC regulations, receiving speed is limited to 53 kbps. Current line noise can impact the speed of the modem.

The V.90 modem WAN connection always uses PPP as the link layer protocol. For correct operation, the link must be connected to a remote access server (RAS).

Business Communications Manager supports the following authentication features:

- Password Authentication Protocol (PAP)
- Challenge Authentication Protocol (CHAP)

Configuring V.90 modem interface for dial up WAN backup connection

The V.90 modem is used for WAN backup connection.

Tips

Remember to set Dial Up global parameters before creating modem dial up interfaces. For information on setting Dial Up global parameters, see "Configuring the Dial Up Global parameters" on page 338.

The same modem maybe shared between the remote dial-in for system administration and the backup WAN link. The WAN backup function is not available if a break in the WAN permanent connection occurs while a system administrator is connected to Business Communications Manager using the V.90 modem.

To configure the V.90 modem interface:

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **V.90** key to see available modem interfaces.
   Business Communications Manager comes with a default modem backup interface called **ModemBackup**.
3. Click the **ModemBackup** heading. The V.90 Summary screen appears.
4. Configure the V.90 Summary parameters according to Figure 151.

Table 151 V.90 modem summary parameters

Attribute	Description
Interface	Shows the name of the modem interface selected.
IP Address	Enter the IP address of the modem interface when it connects. Users can set a fixed IP address for the dial-up interface. If a fixed address is specified, Business Communications Manager uses the address on the receiving end. Users can select **RemoteAssigned** to indicate that Business Communications Manager must obtain an IP address from the remote end and use it. The address obtained depends on the RAS server to which Business Communications Manager connects. The default value is **RemoteAssigned**.

Table 151 V.90 modem summary parameters

Attribute	Description
Description	Shows a description of the interface.
Version	Shows the version of the modem subsystem.
Status	View the modem interface resource status and enable or disable the modem interface. The possible states are: **Up**: The auto WAN backup service is enabled and the dial-up link is currently active. **Down**: The auto WAN backup service is enabled and the dial-up link is currently disconnected. **Enabled**: The interface is enabled for use by the auto-backup server. **Disabled**: The auto WAN backup service is disabled.

5 Press the **Tab** key to save the settings.

6 Click the **V.90 Link Parameters** tab.
The V.90 Link Parameters screen appears.

7 Configure the Modem Link Parameters according to Figure 152.

Table 152 Modem link parameters

Attribute	Description
Telephone Number	Lets you type a telephone number to use to connect using the modem interface. If needed, include area codes and all necessary digits to dial an external number.
Alternate Telephone Number	Lets you type an alternate number to use to connect using the modem interface. Include area codes and all necessary digits to dial an external number.
Connect Rate	Lets you specify the initial speed (in bits per second) for the modem to connect. Set to the maximum permissible value for best results. Permitted values: 57600, 38400, 19200, 9600, 4800. **Note**: This is the initial rate; the actual rate is always negotiated.
Dial Retries	Lets you set the number of attempts the system must make when trying to connect before considering the connection non operational. The default value is **3**.
Dial Interval	Lets you set the interval, in seconds, between successive connection attempts. The default value is **60**.
Speaker Mode	Lets you enable or disable the speaker during initial link establishment.
IP Header Compression	Lets you enable or disable IP header compression. To function, the receiving end must also use this feature.
Software Compression	Lets you enable or disable data compression in the software, instead of the modem. For dial-up connections, Unified Manager uses Microsoft Point-to-Point Compression algorithm (MPPC).
Hardware Compression	Lets you enable or disable data compression in the hardware instead of the software.
PPP LCP Extensions	Lets you enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.

8 Press the **TAB** key to save the settings.

9 Click the **V.90 Access Parameters** tab.
The V.90 Access Parameters screen appears.

10 Configure the V.90 Modem Access Parameters according to Figure 153.

Table 153 V.90 modem access parameters

Attribute	Description
Authentication	Lets you select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: The Challenge Handshake Authentication Protocol (CHAP) is used first and if the receiving end of the link declines, PAP is used to authenticate the link. **EncryptedOnly**: Only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Lets you enable or disable link authentication in both directions. The default value is **Disabled**.
User ID (name password)	Lets you define a user name and a password that the link uses to authenticate itself when dialing out to another router.

11 Press the **TAB** key to save the settings.

ISDN Dial Up

Business Communications Manager supports ISDN Dial Up for dial-on-demand WAN access. You have the choice to use ISDN BRI/PRI as a persistent or dial-on-demand WAN connection or as a back up for your permanent WAN connection.

Tips

To use an ISDN dial-up connection, you must first configure your system for ISDN. For more information, refer to Appendix B, "ISDN Overview," on page 557. If your system is already configured to support ISDN, make sure you configure a Data Module for ISDN dial up connection. For more information, see "Configuring a data module" on page 350.

After you have created an ISDN dial up interface, you must use "Net Link Manager" on page 412 to select which type of network connection the system must use for primary and backup connection.

Creating an ISDN dial up interface

1 On the navigation tree, click the **Resources** key, and click the **Dial Up** key.

2 Click the **ISDN** heading.

3 Click the **Add** button.
Or, right click the **ISDN** heading and click **Add**.
The Add ISDN dialog box appears.

4 In the **(Dial In) Name** box, type the name of the interface you are creating.
This is the name a dial in user must enter to access this interface.

Caution:
If you are creating an ISDN interface to use as a backup for a permanent WAN connection, the **(Dial In) Name** must contain the string “backup”. For example, “ISDNbackup” is a valid name if you want to use an ISDN connection as a WAN backup connection.

5 In the **Password** box, type a password.
This is the password a dial in user must enter to access this interface.

6 In the **Confirm Password** box, type the password again.

7 In the **Channel** list, select the channel the connection must use.

8 Click **Save** to save your settings.
The newly created ISDN interface appears under **ISDN**.

Configuring an ISDN interface

To configure an ISDN interface:

1 On the navigation tree, click the **Resources** key and click the **Dial Up** key.

2 Click the **ISDN** key and click on the interface you want to configure.
The ISDN Summary screen appears.

3 Configure the ISDN Summary settings according to Figure 154.

Table 154 ISDN summary settings

Attribute	Description
Interface	Shows the name of the ISDN interface selected.
IPAddress	Enter the IP address of the ISDN interface when it connects. You can set a fixed IP address for the dial-up interface or you can select **RemoteAssigned** to indicate that Business Communications Manager must obtain an IP address from the remote end. The address obtained depends on the RAS server to which Business Communications Manager connects. The default value is **RemoteAssigned**.
Description	Shows a description of the interface.
Version	Show the version number of the interface.
Status	Lets you view and set the ISDN interface resource status. Possible values are: **Connect**: The ISDN interface is currently connected. Also used to force the interface to initiate a connection. **Disconnect**: The ISDN interface is not currently connected. **Enabled**: The ISDN interface is enabled for use. **Disabled**: The ISDN interface is disabled.

Tip
You cannot select an ISDN interface that is set to “RemoteAssigned” as the Local Gateway IP for the VoIP Gateway.

4 Press the **TAB** key to save the settings.

5 Click the **ISDN Link Parameters** tab.
The ISDN Link Parameters screen appears.

6 Configure the ISDN Link Parameters according to Figure 155.

Table 155 ISDN link parameters

Attribute	Description
Dial Retries	Enter the number of times the systems attempts to connect before considering the connection non operational. The default value is **3**.
Dial Interval	Enter the interval, in seconds, between connection attempts. The default value is **60**.
IP Header Compression	Enable or disable IP header compression. The feature must be enable at both ends of the connection. The default value is **Enabled**.
Software Compression	Enable or disable software compression. When enabled, all dial-up connections use Microsoft Point-to-Point Compression (MPPC). The default value is **Disabled**.
PPP LCP Extensions	Enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.
Disconnect Time	Enter the interval, in seconds, during which the ISDN interface disconnects when there is no traffic. If you select **PersistentConnection**, the ISDN interface will not disconnect.
DNS Address 1	Enter the IP address of the Primary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server. **Note**: If you select **NoNameServerAddressesUsed**, this setting is automatically set in DNS Address 2 box.
DNS Address 2	Enter the IP address of the Secondary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server.
Protocol	Select the protocol that this ISDN interface uses.You can choose **TCP/IP**, **IPX** or **Both**.

7 Press the **TAB** key to save the settings.

8 Click the **ISDN Access Parameters** tab.
The ISDN Access Parameters screen appears.

9 Configure the ISDN Access Parameters according to Figure 156.

Table 156 ISDN access parameters

Attribute	Description
Authentication	Select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: When selected, the Challenge Handshake Authentication Protocol (CHAP) is used first and if the receiving end of the link declines,PAP is used to authenticate the link. **EncryptedOnly**: When selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Enable or disable link authentication in both directions. The default value is **Disabled**.

10 Press the **TAB** key to save the settings.

11 Click the **ISDN Dial-Out User** tab.
The ISDN Dial-out User screen appears.

12 On the **Configuration** menu, click **Modify ISDN Dial-out User**.

13 Configure the ISDN Dial-out User parameters according to Figure 157.

Table 157 ISDN dial-out user parameters

Attribute	Description
User Name	Enter the user name that the link must use to authenticate itself when dialing out to another router.
Password	Enter the password that the link must use to authenticate itself when dialing out to another router.

14 Click the **Save** button.

15 Click the **ISDN Channel Characteristics** tab.
The ISDN Channel Characteristics screen appears.

ISDN Channel Characteristics

To add an ISDN channel to the ISDN Channel Characteristics list

1 On the **Configuration** menu, click **Add ISDN Channel.**
The ISDN Channel Characteristics screen appears.

2 Configure the ISDN Channel Characteristic according to Figure 158.

Table 158 ISDN channel characteristics

Attribute	Description
Row (R#)	Identifies the number of the item in the ISDN channel list.
Port	Shows the channel selected for this ISDN interface. The channel shown here is the channel you selected when you created the ISDN interface.

Table 158 ISDN channel characteristics (Continued)

Attribute	Description
Phone 1	Enter the phone number to use to make an ISDN connection to the network or to Business Communications Manager. If needed, include area codes and all necessary digits to dial an external number. The phone number must contain only numerical digits only (no alphabetical or other characters are allowed).
Phone 2	Enter an alternate phone number to use to make the ISDN connection. If needed, include area codes and all necessary digits to dial an external number. The phone number must contain numerical digits only (no alphabetical or other characters are allowed).
Line Type	Select a 64K or 56K digital line.
Fallback	Choose whether or not to fall back to a slower speed if unable to connect at the previously set speed.

3 Click the Save button.

To modify the characteristics of an existing ISDN channel:

1 Click the ISDN Channel Characteristic you want to modify.

2 On the **Configuration** menu, click **Modify ISDN Channel.**
The ISDN Channel Characteristics screen appears.

3 Make the necessary changes.

4 Click the **Save** button to save your settings.

To delete an ISDN channel from the ISDN Channel Characteristics list:

1 Click the ISDN Channel Characteristic you want to delete.

2 On the **Configuration** menu, select **Delete ISDN Channel.**
A confirmation dialog box appears.

3 Click the **Yes** button.

Deleting an ISDN interface

To delete an ISDN interface:

1 On the navigation tree, click the **Resources** key and click the **Dial Up** key.

2 Click the **ISDN** key.

3 Click the heading of the ISDN interface you want to delete.

4 Click the **Delete** button.
Or, right click the ISDN interface heading and click **Delete**.
A confirmation dialog box appears.

5 Click **Yes**.

Point to Point Protocol on Ethernet (PPPoE)

PPPoE is the protocol Business Communications Manager uses for a dial-up connection using a Digital Subscriber Line (DSL) connection.

Enabling PPPoE

PPPoE does not appear on Unified Manager until you enable it.

To enable PPPoE:

1. Launch your web browser.
2. In the URL address field, type the Business Communications Manager IP address, including the port number 6800.
   For example: *HTTP://10.10.10.1:6800*

   Note: You must include **HTTP://** with the address and port number to access Unified Manager when you are using Internet Explorer as your browser.

   The Business Communications Manager Unified Manager initial page appears.
3. Click the **Maintenance** button.
   The Network Password screen appears.
4. In the **User Name** box, type the system administrator user name.
   The default system administrator user name is *supervisor.*
5. In the **Password** box, type the system administrator password.
   The default system administrator password is *visor.*
6. Click the **OK** button.
   The Product Maintenance & Support screen appears.
7. Click the **Install Optional Components** link.
   The Install Optional Components screen appears.
8. Click the **PPPoE** link.
   The PPPoE install wizard starts.
9. Follow the prompts on the screen to enable PPPoE.

   The PPPoE install wizard consists of three steps. Business Communications Manager reboots after each step.
   It takes 10 to 15 minutes to enable PPPoE.

Creating a PPPoE dial up interface

1. On the navigation tree, click the **Resources** key, and click the **Dial Up** key.
2. Click the **PPPoE** heading.
3. Click the **Add** button.
   Or, right click the **PPPoE** heading and click **Add**.
   The Add PPPoE dialog box appears.
4. In the **(Dial In) Name** box, type the name of the interface you are creating.
5. In the **Password** box, type a password.
6. In the **Confirm Password** box, type the password again.
7. In the **Interface** list, select the LAN interface that connects to the DSL modem.
8. Click **Save** to save your settings.
   The newly created PPPoE interface appears under **PPPoE**.

Configuring PPPoE

To configure a PPPoE interface:

1. On the navigation tree, click the **Resources** key and click the **Dial Up** key.
2. Click the **PPPoE** key and click on the interface you want to configure.
   The PPPoE Summary screen appears.
3. Configure the PPPoE Summary settings according to Figure 154.

Table 159 PPPoE summary settings

Attribute	Description
Interface	Shows the name of the PPPoE interface selected.
IPAddress	Select **RemoteAssigned** to indicate that Business Communications Manager must obtain an IP address from the remote end. The default value is **RemoteAssigned**.
Description	Shows a description of the interface.
Version	Show the version number of the interface.
Status	Lets you view and set the PPPoE interface resource status. Possible values are: **Connect**: The PPPoE interface is currently connected. Also used to force the interface to initiate a connection. **Disconnect**: The PPPoE interface is not currently connected. **Enabled**: The PPPoE interface is enabled for use. **Disabled**: The PPPoE interface is disabled.

4. Press the **TAB** key to save the settings.
5. Click the **PPPoE Link Parameters** tab.
   The PPPoE Link Parameters screen appears.

6 Configure the PPPoE Link Parameters according to Figure 155.

Table 160 PPPoE link parameters

Attribute	Description
Dial Retries	Enter the number of times the systems attempts to connect before considering the connection non operational. The default value is **3**.
Dial Interval	Enter the interval, in seconds, between connection attempts. The default value is **60**.
IP Header Compression	Enable or disable IP header compression. The feature must be enable at both ends of the connection. The default value is **Enabled**.
Software Compression	Enable or disable software compression. When enabled, all dial-up connections use Microsoft Point-to-Point Compression (MPPC). The default value is **Disabled**.
PPP LCP Extensions	Enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.
Disconnect Time	Enter the interval, in seconds, during which the PPPoE interface disconnects when there is no traffic. If you select **PersistentConnection**, the PPPoE interface will not disconnect.
DNS Address 1	Enter the IP address of the Primary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server. **Note**: If you select **NoNameServerAddressesUsed**, this setting is automatically set in DNS Address 2 box.
DNS Address 2	Enter the IP address of the Secondary DNS server that this interface will use. Select **NoNameServerAddressesUsed** if you do not want this interface to use a DNS server.
Protocol	Select the protocol that this PPPoE interface uses.You can choose **TCP/IP**, **IPX** or **Both**.

7 Press the **TAB** key to save the settings.

8 Click the **PPPoE Access Parameters** tab.
The PPPoE Access Parameters screen appears.

9 Configure the PPPPoE Access Parameters according to Figure 156.

Table 161 PPPoE access parameters

Attribute	Description
Authentication	Select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: When selected, the Challenge Handshake Authentication Protocol (CHAP) is used first and if the receiving end of the link declines,PAP is used to authenticate the link. **EncryptedOnly**: When selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Enable or disable link authentication in both directions. The default value is **Disabled**.

10 Press the **TAB** key to save the settings.

11 Click the **PPPoE Dial-Out User** tab.
The PPPoE Dial-out User screen appears.

12 Click the PPPoE Dial-out User you want to modify.

13 On the **Configuration** menu, click **Modify PPPoE Dial-out User**.

14 Configure the PPPoE Dial-out User parameters according to Figure 157.

Table 162 PPPoE dial-out user parameters

Attribute	Description
User Name	Enter the user name that the link must use to authenticate itself when dialing out to another router.
Password	Enter the password that the link must use to authenticate itself when dialing out to another router.

15 Click the **Save** button.

16 Click the **PPPoE Channel Characteristics** tab.
The PPPoE Channel Characteristics screen appears.

17 Configure the PPPoE Channel Characteristic according to Figure 158.

Table 163 PPPoE channel characteristics

Attribute	Description
Row (R#)	Identifies the number of the item in the PPPoE channel list.
Port	Shows the channel selected for this PPPoE interface. The channel shown here is the channel you selected when you created the PPPoE interface.

Deleting an PPPoE interface

To delete an PPPoE interface:

1 On the navigation tree, click the **Resources** key and click the **Dial Up** key.

2 Click the **PPPoE** key.

3 Click the heading of the PPPoE interface you want to delete.

4 Click the **Delete** button.
Or, right click the PPPoE interface heading and click **Delete**.
A confirmation dialog box appears.

5 Click **Yes**.

Guidelines for using Remote Dial-in

Consider the following guidelines when using remote dial-in:

- The remote dial-in for administration and the backup WAN link share the same modem. If a remote administration user is connected while the primary link breaks, the automatic backup function does not occur.
- While using the back-up interface, Business Communications Manager always calls. Business Communications Manager does not answer an incoming call from a router on the V.90 interface.
- If you are using the remote dial-in for maintenance, Nortel Networks recommends that you use the Preinstall Client Access Home Page to access Business Communications Manager.

Configuring a data module

Module 8 is reserved for configuring circuit switched B-channels as a WAN interface for the Business Communications Manager. This allows the Integrated QoS Routing feature to create one or more dial up ISDN connections via the PSTN network using PRI or BRI trunks. Business Communications Manager automatically configures the Module type as a Data Module and sets the Data module type to Baystack. Baystack is the only setting supported on Business Communications Manager.

Viewing the data module settings

Use the following procedure to view the current settings for the data module.

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** heading.
   The Bus 08 screen appears.

Programming the BayStack settings

When you select the BayStack data module, the following configuration settings appear:

- Fixed access
- Switched access
- Line assignment
- Line pool access

Fixed access

Fixed access is supported for the Norstar Data Interface (NDI) only. To assign one or more Fixed lines to the data module:

1. Enter the number of the interface to which you need to assign lines.
2. Enter the number of the Fixed line you need to assign to the interface.
3. Select **Unassigned** or **Assigned**.
4. Record each channel and line combination. Each channel used by the BayStack data module maps to a line.

Switched access (PRI & BRI)

You can assign ISDN lines to the BayStack data module to provide:

- normal data network access for the data module
- dial-up backup and overflow bandwidth (additional channels or trunks) as needed

The line assignment and line pool access settings appear in **Switched access**.

Line assignment

You can assign one or more lines to the BayStack data module for incoming data transmission.

Note: The data module will answer data calls only. It will not answer voice calls.

To add line assignments

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** key and click the **Data Module** key.
3. Click the **Line assignment** heading.
4. Click the **Add** button.
   Or, right click the **Line assignment** heading and click **Add**.
   The Add Line assignment screen appears.
5. In **Line** box, enter the number of the trunk or a target line you need to assign to the BayStack data module.
6. Click the **Save** button.
7. Click the heading for the line you added.
8. In the **Dial-in number** box, enter the Dial-In Number for the line (up to 24 digits). The number must match the Dial-In Number entered for the line and channel in BayStack data module programming.
9. Assign additional lines to the BayStack data module as required.

To delete line assignments

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** key and click the **Data Module** key.
3. Click the **Line assignment** key and click the heading for the line you want to delete.
4. Click the **Delete** button.
   Or, right click the heading for the line assignment you want to delete and click **Delete**.
   A confirmation dialog box appears.
5. Click the **Yes** button.

Line pool access

You can give the BayStack data module access to a line pool for outgoing data transmission.

To add line pool access

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** key and click the **Data Module** key.
3. Click the **Line pool access** heading
4. Click the **Add** button.
   Or, right click the **Line pool access** heading and click **Add**.
   The Add Line pool access screen appears.
5. In **Pool** box, enter the letter of the line pool to provide access to the BayStack data module.

   You must program line pool access when you select the switched access settings for the BayStack data module. To use PRI line pools, program the BayStack data module to use a destination code.
6. Click the **Save** button.

To delete line pool access

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the **Bus 08** key and click the **Data Module** key.
3. Click the **Line pool access** key and click the heading for the line pool you want to delete.
4. Click the **Delete** button.
   Or, right click the heading for the line pool you want to delete and click **Delete**.
   A confirmation dialog box appears.
5. Click the **Yes** button.

Chapter 17
Configuring Business Communications Manager Data Services

This chapter describes the programming procedures for the many Business Communications Manager Services, from Telephony to Firewall Filters. Note that a number of other programming steps are also required to get the system up and running.

Programming Data Services

You can configure Services attributes under the following headings in the **Services** section of Unified Manager:

- "DHCP" on page 354
- "DNS" on page 372
- "IP Routing" on page 374
- "IPX Routing" on page 384
- "SNMP" on page 403
- "QoS monitor" on page 408
- "Web cache" on page 410
- "Net Link Manager" on page 412
- "Alarm Service" on page 415
- "NAT (Network Address Translation)" on page 416
- "NTP Client settings" on page 422
- "Virtual Private Networks (VPN)" on page 425
- "Policy-enabled networking" on page 447

DHCP

Business Communications Manager provides DHCP (Dynamic Host Configuration Protocol) service to branch office clients. This service dynamically assigns IP addresses to branch office computers or IP telephones, so you do not need to manually assign an IP address.

To configure Business Communications Manager as your DHCP server, you must create a scope of IP addresses for each LAN interface and then allocate a block of IP addresses to that scope. If you already have a DHCP server then you need to set up Business Communications Manager as a relay agent to that server.

Caution: Check with your network administrator before enabling DHCP. Enabling DHCP on a network that already has a DHCP server can cause problems on the network.

Tips

Because Business Communications Manager retrieves default DHCP parameters from the LAN interface parameters, you must configure a LAN interface before you configure the DHCP server for that interface. For information on configuring a LAN interface, see "LAN" on page 320.

You must define one DHCP scope for each LAN interface. For DHCP service, there are global attributes that affect all scopes and there are attributes that are specific for each scope.

Tip

Use the Business Communications Manager DHCP default configuration unless your network does not allow it.

If you must modify the DHCP default configuration on Business Communications Manager, make sure configuration settings are consistent throughout the network and take the following into consideration:

- If a change in the DHCP configuration resulted in a change in the IP addresses of a scope, perform one of the following actions to ensure good system operation:
  - Execute *ipconfig/release* and *ipconfig/renew* on each of the workstations. For Windows 95 and Windows 98, use the *winipcfg*.
  - For clients that do not support *ipconfig* and *winipcfg* (for example, IP telephones), a reboot is necessary to renew their IP addresses.
- If you made a change in the DNS server configuration or DNS name field, repeat the actions stated in the previous step to ensure proper connectivity with the network.
- Always schedule a down time when making changes to the Business Communications Manager DHCP server configuration to minimize impact on your network users.

Configuring the DHCP Mode

You can configure Business Communications Manager as your DHCP server or as a DHCP Relay Agent by setting the DHCP Mode. To set the DHCP Mode:

1. On the navigation tree, click the **Services** key and click the **DHCP** heading.
   The Summary screen appears.
2. Click the **DHCP Mode** tab.
   The DHCP Mode screen appears.
3. Click the DHCP box and click **DHCPRelayAgent** or **DHCPserver**.
   The default is DHCPserver.
4. Press the **Tab** key to save the settings.

Configuring a DHCP server

If you chose DHCPServer as the DHCP mode, configure the DHCP server settings in the Global Options and Summary screen.

1. On the navigation tree, click the **Services** key and click the **DHCP** heading.
   The Summary screen appears.
2. Click the **Global Options** tab.
   The Global Options screen appears.
3. Configure the Global Options attributes. These attributes are described in the following table.

Setting	Definition
IP Domain Name	This setting defaults to the value entered in the **Domain** box of the DNS Summary page (see "DNS" on page 372) because all the DHCP clients of Business Communications Manager are in the same DNS domain as the Business Communications Manager server. Business Communications Manager runs only a DNS cache and does not introduce another DNS zone. The domain name is passed to the client when Business Communications Manager responds to a client's DHCP requests. Use caution if you change this.
WINS Node Type	Allows you to specify a client's WINS node type. Business Communications Manager automatically sets this value to **8** (indicating H-Node) on all DHCP clients of Business Communications Manager. This setting configures the DHCP client PCs to use p-node name resolution before resorting to b-node name resolution. This is efficient when a WINS server is configured for the network. Business Communications Manager also includes a WINS server. Other options available are: **1**: indicates a b-node that uses a broadcast mechanism for NetBIOS name resolution. **2**: indicates a p-node that uses a point-to-point mechanism involving a WINS Server for NetBIOS name resolution. **4**: indicates a m-node that first uses a broadcast and then a point-to-point mechanism for NetBIOS name resolution. Use caution if you change this.

Setting	Definition
NORTEL IP Terminal Information	Contains vendor specific information for IP telephones. The default value is: Nortel-i2004-A,10.10.10.1:7000,1,250;10.10.10.1:7000,1,250. where: • Nortel-i2004-A - is the identification name for the IP telephone • 10.10.10.1 - is the IP address for the primary Terminal Proxy Server (TPS). This is normally the Published IP address of the Business Communications Manager. • 7000 - is the UDP port number for the TPS (S1) • 1 - is the Initial Action Code for the IP telephone • 250 - is the retry count for attempts to connect to the TPS (S1) • Nortel-i2004-A - is the identification name for the IP telephone • 10.10.10.1 - is the IP address for the backup TPS (S2) • 7000 - is the UDP port number for the TPS (S2) • 1 - is the Initial Action Code for the IP telephone • 250 - is the retry count for attempts to connect to the TPS (S2) **Note**: The S1 and S2 information must be separated by a semi colon (;). The string must be terminated with a period (.).

Note: When you change the published IP address of Business Communications Manager, you must reboot the IP telephones.

4 Press the **Tab** key to save the settings.

Note: Event logging is always on for DHCP server. The event information is recorded in the system admin log.

5 Click the **Summary** tab.
The Summary screen appears.

6 Configure the Summary settings. These settings are described in the following table.

Setting	Definition
Description	Shows the a description of the DHCP service operating on Business Communications Manager.
Version	Shows the version number of the DHCP service.
Status	Allows you to enable or disable the DHCP server. When you disable the DHCP server, you need to assign static IP addresses to the clients or configure DHCP as a Relay Agent to use another DHCP server on the network. The default is Disabled.

7 Press the **Tab** key to save the settings.

LAN settings for DHCPServer

If you configured the DHCP mode for DHCPServer, then configure the LAN scope attributes as follows. If the DHCP mode is DHCPRelayAgent refer to "LAN settings for DHCPRelayAgent" on page 369.

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

Note: If your Business Communications Manager system has multiple LAN interfaces, you can see multiple DHCP scopes under DHCP. They are named LAN1 and LAN2. This section describes configuring DHCP for LAN1. Follow the same instructions to configure the parameters for LAN2.

3 Configure the scope-specific settings. These settings are described in the following table.

Attribute	Description
Name	Allows you to specify the name of the LAN scope.
Description	Allows you to specify a description for the LAN scope.
DNS Server	Allows you to specify the IP address of the DNS server. Business Communications Manager automatically assigns the value for this parameter. If the IP address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
WINS Server	Allows you to specify the IP address of the WINS server. Business Communications Manager automatically assigns the value for this parameter. If the IP address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
Default Gateway	Allows you to specify the IP address of the default next-hop router. Business Communications Manager automatically assigns the value for this parameter. If the IP address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
Lease Time	Allows you to specify the time, in seconds, for an address assignment until the client's lease expires. The default is 259200 seconds (72 hours).
Scope Status	Allows you to enable or disable the scope. The default is enabled.

Note: If the IP address or subnet mask for a LAN interface changes, the system creates or modifies the corresponding DHCP scope for the interface. This operation also involves setting default values for some parameters. By default, Business Communications Manager sets the IP address of the corresponding LAN interface to the DNS Server, WINS Server, Default Gateway options of the scope. It also sets the lease time to three days and creates a range of addresses for the scope. If the IP address of the LAN interface is in the lower half of the subnet, the address range set for the scope includes all the addresses above the LAN interface address. If the IP address of the LAN interface is in the upper half of the subnet, the address range set for the scope includes all the addresses below the LAN interface address. By default, the scope is enabled.

Note: When DNS is disabled in Business Communications Manager, the DNS Server box must be set to the IP address of a remote DNS server.

4 Press the **TAB** key to save the settings.

Address ranges

Address ranges allow you to specify the valid IP addresses for the DHCP clients.

Note: You must add at least one Address range to use DHCP server.

To add an address range:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Address Range** tab.
The Address Range screen appears.

4 On the **Configuration** menu, click **Add Address Range**.
The Address Range dialog box appears.

5 Configure the Address Range attributes. These attributes are described in the following table.

Attribute	Description
Range (R#)	Allows you to specify the Range identifier. The range box uniquely identifies an Address range in the scope. The value for this setting must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the range in the table. For example, 'R2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing range name, it modifies the existing range. If you use nonsequential numbers, the system automatically reassigns sequential numbers. When you modify a range, you cannot change the range name. The range name does not have any significance other than identifying an entry.
Start Address	Allows you to specify a the first IP address in the Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Address Range. Make sure the start address and end address are in the same subnet. Enter the IP address in the dotted format.

6 Click the **Save** button to save the address range.

To modify address ranges:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Address Range** tab.
The Address Range screen appears.

4 Click an address in the Address Range table.

5 On the **Configuration** menu, click **Modify Address Range**.
The Address Range dialog box appears.

6 Modify the Address Range settings.

7 Click the **Save** button.

To delete an address range:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Address Range** tab.
The Address Range screen appears.

4 Click an address range in the Address Range table.

5 On the **Configuration** menu, click **Delete Address Range**.
A dialog box appears asking you to confirm the deletion.

6 Click the **Yes** button.

Note: When you delete or modify an IP Address range it removes any excluded addresses that are in the original address range value.

Excluded addresses

Excluded addresses allow you to specify the IP addresses that are not available to DHCP clients. The excluded addresses are also used to ensure that Static IP addresses are not re-assigned by DHCP.

To add an excluded address range:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Excluded Address** tab.
The Excluded Address screen appears.

4 On the **Configuration** menu, click **Add Excluded Address Range**.
The Excluded Address dialog box appears.

5 Configure the Excluded Address attributes. These attributes are described in the following table.

Attribute	Description
Range (E#)	Allows you to specify the Range identifier. The range setting uniquely identifies an excluded range in the scope. The value for this setting must follow certain conventions. You must type the prefix 'E' followed by a unique number identifying the range in the table. For example, 'E2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing excluded range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify an excluded range, you cannot change the range name. The excluded range identifier does not have any significance, other than uniquely identifying an entry.
Start Address	Allows you to specify a the first IP address in the Excluded Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Excluded Address Range. Enter the IP address in the dotted format.

Note: Make sure the start address and end address are in the same subnet. The excluded address range must be completely contained in an IP address range specified for the subnet.

6 Click the **Save** button.

To modify excluded address ranges:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key and click the **LAN1** heading.
   The LAN Scope Specific Options screen appears.
3. Click the **Excluded Address** tab.
   The Excluded Address screen appears.
4. Click an excluded address range in the Excluded Address Range table.
5. On the **Configuration** menu, click **Modify Excluded Address Range**.
   The Excluded Address dialog box appears.
6. Modify the Excluded Address settings.
7. Click the **Save** button.

To delete an excluded address range:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key and click the **LAN1** heading.
   The LAN Scope Specific Options screen appears.
3. Click the **Excluded Address** tab.
   The Excluded Address screen appears.
4. Click an excluded address range in the Excluded Address Range table.
5. On the **Configuration** menu, click **Delete Excluded Address Range**.
   A message prompts you to confirm the deletion.
6. Click the **Yes** button.

Reserved Addresses

Reserved addresses allow you to assign IP addresses to specific DHCP clients.

To add a reserved address:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Local Scope** key and click the **LAN1** heading.
   The LAN Scope Specific Options screen appears.
3. Click the **Reserved Address** tab.
   The Reserved Address screen appears.
4. On the **Configuration** menu, click **Add Reserve Address**.
   The Reserved Address dialog box appears.

5 Configure the Reserved Address settings. These settings are described in the following table.

Setting	Definition
Range (V#)	Allows you to specify the Range identifier. The range setting uniquely identifies a reserved range in the scope. The value for this setting must follow certain conventions. You must type the prefix 'V' followed by a unique number identifying the range in the table. For example, 'V2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing reserved range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify a reserved range, you cannot change the range name. The reserved range name does not have any significance, other than uniquely identifying an entry.
IP Address	Allows you to specify the IP Address that is reserved for this DHCP client. Enter the IP address in the dotted format.
MAC Address	Allows you to specify the MAC address for the DHCP client this IP address is assigned to. The permitted value is 6 bytes in hexadecimal format.
Client Name	Allows you to specify the name of the DHCP client.
Client Description	Allows you to specify the description that will help to identify the DHCP client this IP address is assigned to.
Lease Expiration Date	Shows the date when this IP address is no longer reserved for the DHCP client.
Lease Expiration Time	Shows the time when this IP address is no longer reserved for the DHCP client.

6 Click the **Save** button.

To delete a reserved address:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The LAN Scope Specific Options screen appears.

3 Click the **Reserved Address** tab.
The Reserved Address screen appears.

4 Click a reserved address in the Reserved Address table.

5 On the **Configuration** menu, click **Delete Reserved Address**.
A message prompts you to confirm the deletion.

6 Click the **Yes** button.

Remote Scope

A remote scope is a remote network (not LAN1 or LAN2) that uses the DHCP server to get IP addresses through a DHCP relay agent.

Adding a remote scope

To add a remote scope:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** heading and click the **Add** button.
   Or, right click the Remote Scope heading and click **Add**.
3. Configure the remote scope settings. These settings are described in the following table.

Attribute	Description
Subnet name	Allows you to specify the name of the remote scope.
Subnet Comment	Allows you to specify a description of the remote scope.
IP Address	Allows you to specify the IP address of the remote scope. Enter the IP address in the dotted format.
Subnet Mask	Allows you to specify the subnet mask for the remote scope. Enter the subnet mask in the dotted format.

4. Click the **Save** button.

Remote scope settings

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Configure the remote scope-specific settings. These settings are described in the following table.

Attribute	Description
Name	Allows you to specify the name of the remote scope.
Description	Allows you to specify a description for the remote scope.
DNS Server	Allows you to specify the IP address of the DNS server.
WINS Server	Allows you to specify the IP address of the WINS server.
Default Gateway	Allows you to specify the IP address of the default next-hop router.
Lease Time	Allows you to specify the time, in seconds, for an address assignment until the client's lease expires.
Scope Status	Allows you to enable or disable the scope.

5. Press the **TAB** key to save the settings.

Address ranges

Address ranges allow you to specify the valid IP addresses for these DHCP clients.

To add an address range:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Click the **Address Range** tab.
   The Address Range screen appears.
5. On the **Configuration** menu, click **Add Address Range**.
   The Address Range dialog box appears.
6. Configure the Address Range attributes. These attributes are described in the following table.

Attribute	Description
Range (R#)	Allows you to specify the Range identifier. The range box uniquely identifies an Address range in the scope. The value for this setting must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the range in the table. For example, 'R2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing range name, it modifies the existing range. If you use nonsequential numbers, the system automatically reassigns sequential numbers. When you modify a range, you cannot change the range name. The range name does not have any significance other than identifying an entry.
Start Address	Allows you to specify a the first IP address in the Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Address Range. Make sure the start address and end address are in the same subnet. Enter the IP address in the dotted format.

7. Click the **Save** button.

To modify address ranges:

1. On the navigation tree, click the **Services** key and click the **DHCP** key.
2. Click the **Remote Scope** key.
3. Click the remote scope you want to modify.
   The Scope Specific Options screen appears.
4. Click the **Address Range** tab.
   The Address Range screen appears.
5. Click an address in the Address Range table.
6. On the **Configuration** menu, click **Modify Address Range**.
   The Address Range dialog box appears.

7 Modify the Address Range settings.

8 Click the **Save** button.

To delete an address range:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Address Range** tab.
The Address Range screen appears.

5 Click an address range in the Address Range table.

6 On the **Configuration** menu, click **Delete Address Range**.
A dialog box appears asking you to confirm the deletion.

7 Click the **Yes** button.

Note: When you delete or modify an IP Address range it removes any excluded addresses that are in the original address range value.

Excluded addresses

Excluded addresses allow you to specify the IP addresses that are not available to DHCP clients. The excluded addresses are also used to ensure that Static IP addresses are not re-assigned by DHCP.

To add an excluded address range:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Excluded Address** tab.
The Excluded Address screen appears.

5 On the **Configuration** menu, click **Add Excluded Address Range**.
The Excluded Address dialog box appears.

6 Configure the Excluded Address attributes. These attributes are described in the following table.

Attribute	Description
Range (E#)	Allows you to specify the Range identifier. The range setting uniquely identifies an excluded range value in the scope. The value for this setting must follow certain conventions. You must type the prefix 'E' followed by a unique number identifying the range in the table. For example, 'E2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing excluded range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify an excluded range, you cannot change the range name. The excluded range name does not have any significance, other than uniquely identifying an entry.
Start Address	Allows you to specify a the first IP address in the Excluded Address Range. Enter the IP address in the dotted format.
End Address	Allows you to specify a the last IP address in the Excluded Address Range. Enter the IP address in the dotted format.

Note: Make sure the start address and end address are in the same subnet. The excluded address range must be completely contained in an IP address range specified for the subnet.

7 Click the **Save** button.

To modify excluded address ranges:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Excluded Address** tab.
The Excluded Address screen appears.

5 Click an excluded address range in the Excluded Address Range table.

6 On the **Configuration** menu, click **Modify Excluded Address Range**.
The Excluded Address dialog box appears.

7 Modify the Excluded Address settings.

8 Click the **Save** button.

To delete an excluded address range:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Excluded Address** tab.
The Excluded Address screen appears.

5 Click an excluded address range in the Excluded Address Range table.

6 On the **Configuration** menu, click **Delete Excluded Address Range**.
A message prompts you to confirm the deletion.

7 Click the **Yes** button.

Reserved Addresses

Reserved addresses allow you to assign IP addresses to specific DHCP clients.

To add a reserved address:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Reserved Address** tab.
The Reserved Address screen appears.

5 On the **Configuration** menu, click **Add Reserve Address**.
The Reserved Address dialog box appears.

6 Configure the Reserved Address settings. These settings are described in the following table.

Setting	Definition
Range (V#)	Allows you to specify the Range identifier. The range setting uniquely identifies a reserved range in the scope. The value for this setting must follow certain conventions. You must type the prefix 'V' followed by a unique number identifying the range in the table. For example, 'V2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing reserved range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify a reserved range, you cannot change the range name. The reserved range name does not have any significance, other than uniquely identifying an entry.
IP Address	Allows you to specify the IP Address that is reserved for this DHCP client. Enter the IP address in the dotted format.
Mac Address	Allows you to specify the MAC address for the DHCP client this IP address is assigned to. The permitted value is 6 bytes in hexadecimal format.
Client Name	Allows you to specify the name of the DHCP client.
Client Description	Allows you to specify the description that will help to identify the DHCP client this IP address is assigned to.

Setting	Definition
Lease Expiration Date	Shows the date when this IP address is no longer reserved for the DHCP client.
Lease Expiration Time	Shows the time when this IP address is no longer reserved for the DHCP client.

7 Click the **Save** button.

To delete a reserved address:

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to modify.
The Scope Specific Options screen appears.

4 Click the **Reserved Address** tab.
The Reserved Address screen appears.

5 Click a reserved address in the Reserved Address table.

6 On the **Configuration** menu, click **Delete Reserved Address**.
A message prompts you to confirm the deletion.

7 Click the **Yes** button.

Deleting a Remote Scope

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Remote Scope** key.

3 Click the remote scope you want to delete.
The Remote Scope Specific Options screen appears.

4 Click the **Delete** button.
Or, right click the remote scope you want to delete and click **Delete**.
A message prompts you to confirm the deletion.

5 Click the **Yes** button.

Configuring a DHCP Relay Agent

If you chose DHCPRelayAgent as the mode, configure the DHCP Relay Agent settings in the Global Options and Server List screens.

1 On the navigation tree, click the **Services** key and click the **DHCP** heading.
The DHCP Mode screen appears.

2 Click the **Global Options** tab.
The Global Options screen appears.

3 Click the **Log Level** box and choose which information is recorded in the system admin log.
Errors Only - records error messages only
Warnings Also - records error message and warning messages
Maximum - records error message, warning messages and event messages
Disabled - disables recording of DHCP messages
The default is **Errors Only**.

4 Click the **Server List** tab.
The Server List screen appears.

5 On the **Configuration** menu, click **Add server**.
The Server List dialog box appears.

6 Type in the IP address of the DHCP server.

Note: You can specify a number of servers. The routing component searches the list for the server on the same subnet as the interface and forwards the DHCP packet.

7 Click the **Save** button.

To delete a server from the Server List:

1 Click a server in the Server List.

2 On the **Configuration** menu, click **Delete server**.
A dialog box appears asking you to confirm the deletion.

3 Click the **Yes** button.

LAN settings for DHCPRelayAgent

If you configured the DHCP mode as DHCPRelayAgent (refer to "Configuring a DHCP Relay Agent" on page 368), then configure the LAN scope attributes as follows. If the mode is DHCPServer refer to "LAN settings for DHCPServer" on page 357.

1 On the navigation tree, click the **Services** key and click the **DHCP** key.

2 Click the **Local Scope** key and click the **LAN1** heading.
The Relay Agent Interface Parameters screen appears.

Note: If your Business Communications Manager system has multiple LAN interfaces, you can see multiple DHCP scopes under DHCP. They are named LAN1 and LAN2. This section describes configuring the DHCP scope for LAN1. Follow the same instructions to configure any of the parameters under the scope for LAN2.

3 Configure the scope-specific settings. These settings are described in the following table.

Attribute	Description
Relay DHCP packets	Allows you to enable or disable the relay of DHCP packets on this interface. The default is disabled.
Hop-count threshold.	Allows you to specify the maximum number of hops. After this number of hops, DHCP requests are discarded. The values are 0 to 16. The default value is 4.
Seconds-since-boot threshold	Allows you to specify the minimum number of seconds since the last boot of Business Communications Manager, before Business Communications Manager forwards DHCP requests. The values are 1 to 3600. The default value is 4.

4 Press the **Tab** key to save the settings.

Importing and Exporting DHCP data

You can export the DHCP data for an interface to a file on the Business Communications Manager system. This saves an image of the current DHCP programming for that interface.

When the IP address of LAN1 or LAN2 changes, the DHCP programming for that interface is lost. To save the DHCP programming, export the DHCP data before you change the IP address of the interface. Then, after you change the IP address, import the DHCP programming for the interface.

Exporting DHCP data

When you export the DHCP data, the following information is save to the file:

- Address Range
- Excluded Address Range
- Reserved Address Range
- Scope options

The DHCP data is stored on the Business Communications Manager in the directory D:\Data Files\Nortel Networks\Unified Manger. The file is named *ScopeName.dat* where ScopeName is the name of the DHCP scope.

To export the DHCP data:

1 On the navigation tree, click the Services key and click the DHCP key.

2 Click the **Local Scope** key to export data for a local scope.
Click the **Remote Scope** key to export data for a remote scope.

3 Click the scope from which you want to export data.

4 On the **Tools** menu, click **Export**.
A confirmation dialog box appears.

5 Click the **Yes** button.

Note: If you have exported the DHCP data for a scope with this name before, the data from this export will overwrite the previous export.

Importing DHCP data

When you import the DHCP data, the DHCP programming from a previous export replaces the current DHCP programming for the scope.

To import the DHCP data:

1 On the navigation tree, click the Services key and click the DHCP key.

2 Click the **Local Scope** key to import data for a local scope.
Click the **Remote Scope** key to import data for a remote scope.

3 Click the scope for which you want to import data.

4 On the **Tools** menu, click **Import**.
A confirmation dialog box appears.

5 Click the **Yes** button.

DNS

Business Communications Manager functions as both a gateway to the Internet and as a DNS proxy.

Note: If your PC is a DHCP client under Business Communications Manager, you do not have to let your workstations know that Business Communications Manager is your Internet gateway.

When Business Communications Manager receives DNS requests from clients, it first checks its local cache for name entries and records. If found locally, Business Communications Manager immediately responds to clients. Otherwise, Business Communications Manager creates a new DNS request to the remote Primary or Secondary DNS servers on behalf of the client. If the remote DNS server responds with the requested records, they are forwarded to clients and cached in Business Communications Manager.

Note: If you use the Quick Install Wizard, DNS proxy is enabled by the wizard.

Guidelines for using Business Communications Manager DNS service

Consider the following guidelines when using DNS:

- If you enable the Business Communications Manager DNS service, make sure that you configure each workstation on the network to use Business Communications Manager as DNS server.
- When you disable Business Communications Manager DNS service, set the DNS Server field in DHCP configuration to the remote DNS server IP address. If DHCP service is also disabled in Business Communications Manager, you must configure each workstation on your network to use the remote DNS server.

To configure DNS services settings

1 On the navigation tree, click the **Services** key and click the **DNS** heading.
The DNS Summary screen appears.

2 Configure the DNS Summary attributes. These attributes are described in the following table.

Attribute	Description
Description	Allows you to view the description of the DNS server.
Version	Allows you to view the version of the DNS service.
Status	Allows you to enable or disable the DNS cache proxy in Business Communications Manager.
IP Domain	Allows you to specify the domain name that Business Communications Manager and its DHCP clients uses. When you modify the Domain, the setting automatically copies to **Domain Name** global options under **DHCP** service.

Attribute	Description
Primary (and Secondary) Server	Allows you to specify the IP addresses of the primary DNS server and the secondary DNS server in a valid dot format. When you specify a secondary DNS server, separate the two IP addresses by a space. The DNS cache uses the servers in the order you specify, so make sure the IP address secondary DNS server appears second.
Forward Timeout	Allows you to specify the time-out, in seconds, to resolve queries using the DNS servers that you specify in DNS server.

3 Press the **Tab** key to save the settings.

Note: The DNS proxy carries security features because it keeps all of the internal IP addresses from external web servers. For information on other security features, see "NAT (Network Address Translation)" on page 416 and "IP Firewall Filters" on page 470.

IP Routing

The **IP Routing** service setting allows you to select, add or delete routing protocol on specific interfaces, choose routing protocol options, and add or delete static routes.

Note: If you change the IP address or subnet mask of any interface (LAN or WAN), you must reboot Business Communications Manager before you configure IP routing.

Business Communications Manager supports the following IP routing protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

Routing Information Protocol (RIP)

Business Communications Manager supports RIP, a widely-used protocol for managing routing information in a self-contained network, such as a corporate intranet. RIP measures the shortest path between two points on a network in terms of the number of hops between those points.

Business Communications Manager router sends RIP routing information updates that list all the other hosts it knows about, to its nearest neighbor host every 30 seconds. The neighbor host sends the information to its next neighbor, until all the hosts in the network know the routing paths, a state known as network convergence. RIP uses a hop count to determine network distance. Each router in the network uses the routing table information to determine the next host for the packet, until it reaches the destination.

Business Communications Manager supports on demand routing table update and periodic routing table update. On demand routing table update is available only on demand-dial interfaces. Periodic update operates efficiently on persistent links

Business Communications Manager supports IP Subnet Aggregation, or Subnet Summary, in RIP v2. This feature is turned on by default.

When Subnet Aggregation is on and there are two or more subnets with common leading digits in their subnet addresses, RIP v2 will summarize these subnets and advertise a single aggregated entry to its neighboring routers.

For information on how to select RIP as your routing protocol, see “Configuring IP Routing” on page 375.

Open Shortest Path First (OSPF)

Open Shortest Path First protocol bases its path descriptions on “link states” that take into account additional network information. OSPF also lets the user assign cost metrics to a given host router so that some paths are given preference. OSPF supports a variable network subnet mask so that a network can be subdivided into areas. For information on how to select OSPF as your routing protocol, see “Configuring IP Routing” on page 375.

The implementation of OSPF on Business Communications Manager is designed to operate as an edge router in an OSPF intranet, or as a backup router in a small network. Do not configure Business Communications Manager for multiple OSPF areas.

Note: Business Communications Manager is an edge router and will not act as a router spanning RIP and OSPF routing networks (RIP or OSPF redistribution).

Warning: Because OSPF is a “link-state” based routing protocol, you must not use OSPF on dial-on-demand interfaces. Frequent link status (between “up” and “down”) may cause the protocol to become unstable.

Configuring IP Routing

The followings table shows the Business Communications Manager IP routing protocols and the precedence order when conflicting or redundant routes occur.

Precedence	IP Routing Protocols	
1.	Static Routing	
2.	OSPF	RIP v1 and v2

IP Routing global settings

To configure global settings for IP Routing:

1. On the navigation tree, click the **Services** key and click the **IP Routing** heading. The IP routing Summary screen appears.
2. Configure the Routing Summary attributes. These attributes are described in the following table.

Attribute	Description
Description	Shows a description of the router.
Version	Shows the version of the router.
Status	Allows you to enable or disable the router. The possible values are: **Up**: the IP router is currently functioning. **Enabled**: allows you to enable the router. **Disabled**: allows you to disable the router.

Setting the RIP Global Settings

If your network uses RIP, configure the RIP Global Settings as described below. If your network uses OSPF, refer to "Setting the OSPF Global Settings" on page 376.

1 Click the **RIP Global Settings** tab.
The RIP Global Settings screen appears.

2 Configure the RIP Global Settings. These settings are described in the following table.

RIP Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
Triggered Update Interval	Allows you to specify the minimum interval, in seconds, at which a router must send a routing table update if the metric for a given route changes. If the router detects a change in the routing information, the router sends an update message at the specified interval. Possible values are **1** to **50000**. The default value is **5.**

3 Press the **TAB** key to save your settings.

Setting the OSPF Global Settings

If OSPF is the routing protocol of your choice, configure the OSPF Global Settings as described below.

1 Click the **OSPF Global Settings** tab.
The OSPF Global Settings screen appears.

2 Configure the OSPF Global Settings according to the table below.

Attribute	**Description**
OSPF Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
Router ID	Allows you to specify the IP address that uniquely identifies the Business Communications Manager router on your network.

Attribute	Description
Router Area ID	Allows you to specify the area where your Business Communications Manager router is located on your network. The default value is **0.0.0.0**.
Authentication Type	Allows you to enable or disable password authentication. Values are **None**, **Password**. The default value is **None**. For information on how to set the authentication password, see "Configuring OSPF Parameters on a network interface" on page 379.

3 Press the **TAB** key to save your settings.

Configuring IP routing on an interface

After you configured the IP Routing global settings, you must configure each available network interface to use the routing protocol of your choice or static routes.

Note: You must use the same routing protocol on all interfaces. For example, you can not configure your LAN1 interface to use RIP and your WAN1 interface to use OSPF.

This section provides instructions on how to configure interfaces for IP routing and how to create static routes. The available interfaces appear under the **IP Routing** heading. Follow the same instructions to configure all interfaces. For information on how to create static routes, see "Static routes" on page 382.

Configuring RIP parameters on a network interface

1 On the navigation tree, click the **Services** key and click the **IP Routing** key.
The available interfaces for IP routing are listed under the **IP Routing** heading.

2 Click the interface you want to configure.
The Summary window appears. The **Routing Protocol** box shows the current routing protocol.

Tips
If you are changing the routing protocol from OSPF to RIP, you must first set the **Routing Protocol** under each available interface to **None** before you can select **RIP**.

Note: The RIP Parameters window does not appear unless you choose RIP as your routing protocol.

3 In the **Routing Protocol** list, click **RIP**.

4 Press the **Tab** key.
The RIP Parameters tab appears.

5 Click the **RIP Parameters** tab.
The RIP Parameters window appears.

6 Configure the RIP Parameters. These parameters are described in the following table.

Attribute	Description
Metric	Allows you to assign a cumulative value (in terms of hop count or associated cost [if applicable]) to routes passing through this interface. The routing manager adds the metric value of all routes learned through this interface to the metric value of this interface to make routing decisions. The possible values are **1** to **16**. Because RIP protocol can handle up to 15 hop counts before reaching destination, a value of **16** corresponds to “counting to infinity”. The default value is **1**.
Routing Table Update Mode	Allows you to specify the routing table update mode. The possible values are: **On Demand:** The router sends its table when another established router requests it. **Periodic**: The router sends its table to other established router at regular intervals. On dialup interfaces, you must set the Update Mode to **Periodic** to receive updates. The default value is **Periodic**.
Route Announcement Type	Allows you to set the type of routing table update announcements the Business Communications Manager router sends to other routers. The possible values are: **Disabled**: disables sending RIP routing update. If you choose **Disabled**, you must configure the other routers in the subnet to use static routes to access the Business Communications Manager server. **RIP 1**: sends only announcements of RIP v1 type in broadcast mode. **RIP 1 Compatible**: sends RIP v1 and RIP v2 packets in broadcast mode. Use this for a network environment that uses RIP v1 and RIP v2. **RIP 2**: sends RIP v2 packets in multicast mode only. Use this type of announcement only if all other routers connected to the Business Communications Manager server support RIP v2. The default value is **RIP 1**.
Route Accept Type	Allows you to set the type of routing table update announcements the Business Communications Manager router accepts from other routers. The possible values are: **Disabled**: disables sending RIP routing table update announcements. If you choose **Disabled**, you must create static routes in the Business Communications Manager server to access other networks connected to this interface. This method is preferable if you want to keep the routing table small in the Business Communications Manager server. **RIP 1**: accepts only announcements of RIP **1** type. **RIP 1 Compatible**: accepts announcements of RIP 1 and RIP 2 types. **RIP 2**: accepts announcements of RIP 2 type only. The default value is **RIP 1**.
Route Expiration Interval	Allows you to define the period of time within which a route in the routing table must be updated to remain a valid route. The possible values are **15** to **259200** seconds**.** The default value is **180** seconds.
Route Removal Interval	Allows you to define the period of time (in seconds) an invalid route remains in the routing table before the routing manager removes it from the routing table. The possible values are **15** to **29200** seconds**.** The default value is **180** seconds

Attribute	Description
Route Announcement Interval	Allows you to set the time interval (in seconds) between routing table updates when the **Routing Table Update Mode** is set to **Periodic**. The possible values are **5** to **84200** seconds. The default value is **30** seconds.
Route Tag	Allows you to create a special tag which identifies routes announced over the interface. The route tag helps identify route packets when debugging routing problems using a network sniffer.
Poisoned Reverse	Allows you to enable or disable options designed to avoid routing problems such as loops or metric values exceeding the maximum of 15 hop counts. The following options are available: **Actual**: A routing table update process where a routing table update going out repeats the information sent by the originator. The system tries to solve this state known as a loop involving two routers by sending more routing updates. **Split** (split horizon): A routing table update process designed to avoid sending the same routing information back to the originator. **Poisoned**: A routing table update process designed to advertise unreachable routes as having metric value of 16 regardless of incoming routing update information. The default value is **Split**.
Triggered Updates	Allows you enable immediate route update announcements whenever a metric or other information changes in the routing table entries. When **Triggered Updates** is set to **Enabled**, the system gathers new routing information for the period of time defined in the **Triggered Update Interval** from the RIP Summary window (see "IP Routing global settings" on page 375). Triggered updates results in more frequent, smaller RIP routing table updates. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.
Announce Default Route	Allows you to enable or disable the announcement of default routes in incoming route announcements. Use caution when you enable this feature, because improper configuration causes a loss of network connectivity. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.
Accept Default Route	Allows you to enable or disable the acceptance of incoming default routes announcement. Sets default routes as static routes. If you run Net Link Manager to automatically backup the primary WAN link using a dial-up link, Net Link Manager manages the default routes and the default routes that you add are non-operational as soon as a primary link breaks or comes up again. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.

7 Press **Tab** to save your settings.

Configuring OSPF Parameters on a network interface

1 On the navigation tree, click the **Services** key and click the **IP Routing** key.
The available interfaces for IP routing are listed under the **IP Routing** heading.

2 Click the interface you want to configure.
The Summary window appears. The **Routing Protocol** box shows the current routing protocol.

Warning: Because OSPF is a “link-state” based routing protocol, you must not use OSPF on dial-on-demand interfaces. Frequent link status changes (between “up” and “down”) may cause the OSPF protocol to become unstable.

3 In the **Routing Protocol** list, click **OSPF**.

Tips
If you are changing the routing protocol from RIP to OSPF, you must first set the Routing Protocol under each available interface to None before you can select OSPF.

4 Click the OSPF Parameters tab.
The OSPF Parameters screen appears.

Note: The OSPF Parameters tab does not appear unless you choose OSPF as your routing protocol.

5 Configure the OSPF parameters. These parameters are described in the following table.

Attribute	Description
Metric	This field allows you to assign the link cost for this interface that advertised in the router's link state advertisement for this interface. The Metric is an indication of the cost of the route. If multiple routes exist on a network ID, the Metric is used to decide which route is taken. The route with the lowest Metric is the preferred route. If you enter a high number for the Metric, this interface will not be used as much as an interface with a lower Metric. The possible values are **1** to **32767**. The default value is **1**.
Interface Type	Allows you to select the type of interface that describes your network configuration. The possible values are: **Broadcast**: A broadcast network supports multiple routers and addresses a single physical message to all routers. **P2P**: A point-to-point network joins a single pair of OSPF routers. **NBMA**: A Non-Broadcast-Multi-Access (NBMA) network supports multiple routers and cannot address a single physical message to all routers. The default value is **Broadcast**.
Router Priority	Allows you to assign a priority to the Business Communications Manager router. The possible values are **0** to **255**. A value of 0 indicates that the Business Communications Manager system cannot become the designated router. The default value is **1**.
Transit Delay	Allows you to set (in seconds) the estimated round-trip transit delay in the network connected to the interface. The values are **1** to **3600** seconds. The default value is **1**.

Attribute	Description
Retransmit Interval	Allows you to set the number of seconds the router waits before retransmitting after a time-out occurs. The values are **1** to **3600** seconds. The default value is **1**.
Hello Interval	Allows you to define how frequently the router must send “hello packets” on an interface. The values are **1** to **32767** seconds. The default value is **10**.
Dead Interval	Allows you to set the maximum number of seconds the router waits to receive the next hello before considering the adjacent router as non operational. The values are **1** to **32767** seconds. The default value is **40**.
Poll Interval	Allows you to define the period of time the router must keep sending hello packets to an adjacent router that is considered non operational. The values are **1** to **32767** seconds. The default value is **120**.
MTU	Allows you to specify the Maximum Transmission Unit for this interface. The values are **1** to **10000**. The default value is **1500**.
Password	Allows you to define an authentication password, if you selected **Password** as the authentication type in the **Authentication Type** box on the OSPF Global Parameters window. There is no default value provided because the **Authentication Type** is set to **None** by default.

6 Press the **Tab** key to save your settings.

OSPF NBMA Neighbors

Frame Relay on Business Communications Manager is a Non Broadcast Multiple Access (NBMA) network. NBMA is a network that can connect two or more routers, but has no hardware broadcast capability. For OSPF function properly on a NBMA network, you must configure OSPF to unicast to the IP addresses of the routers on the network. The OSPF NBMA Neighbors screen allows you to enter IP addresses of the NBMA Neighbors.

Note: The OSPF NBMA Neighbors is available only forWAN interfaces.

1 On the navigation tree, click the **Services** key and click the **IP Routing** key.

2 Click the WAN interface you want configure.

3 Click the **OSPF NBMA Neighbors** tab.
The OSPF NBMA Neighbors screen appears.

To add OSPF NBMA Neighbors

1 On the **Configuration** menu, click **Add OSPF Neighbor**.
The OSPF NBMA Neighbors screen appears.

2 Configure the OSPF NBMA Neighbor parameters according to the following table.

Attribute	Description
OSPF Neighbor (ON#)	Allows you to specify the OSPF Neighbor identifier.
Neighbor Address	Allows you to specify the IP address of the neighboring router.
Neighbor Priority	Allows you to specify the priority of the neighboring router. The possible values are **1** to **255**. The default value is **1**.

3 Click the **OK** button.

To modify OSPF NBMA Neighbors

1 Click the OSPF NBMA Neighbor you want to modify.

2 On the **Configuration** menu, click **Modify OSPF Neighbor**.
The OSPF NBMA Neighbors screen appears.

3 Change the OSPF NBMA Neighbor parameters.

4 Click the **OK** button.

To delete OSPF NBMA Neighbors

1 Click the OSPF NBMA Neighbor you want to delete.

2 On the **Configuration** menu, click **Delete OSPF Neighbor**.
A confirmation dialog box appears.

3 Click the **Yes** button.

Static routes

You can add static routes to the Business Communications Manager routing table. Static routes added to the routing table take precedence over dynamic routes.

Note: The default route is managed by Net Link Manager. For information about Net Link Manager, refer to "Net Link Manager" on page 412.

To add a static route to the routing table:

1 On the navigation tree, click the **Services** key and click the **IP Routing** key.

2 Click the interface you want configure.

3 Click the **Static Route** tab.
The Static Route screen appears.

4 On the **Configuration** menu, click **Add Static Route**.
The Static Route dialog box appears.

5 Configure the static route attributes. These attributes are described in the following table.

Attribute	Description
Static Route (SR#)	Assign a number to the static route. For example, the valid static route number for the first static route is SR1. The function of the static route number is to uniquely identify an route. If you add more than one static route, use sequential numbers. If you use the number of an existing static route, the system modifies the existing static route. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a static route, you cannot change the Static Route number.
Destination address	Enter the IP address of the destination network or host.
Destination mask	Enter the subnet mask corresponding to the destination address.
Next Hop Router	Enter the IP address of next hop router.
Metric Value	Enter the metric value associated with the interface. The system adds the metric to the hop count of the routes received through the interface.

6 Click the **Save** button.

To modify the configuration of a static route:

1 Click a static route you want to modify in the Static Route table.

2 On the **Configuration** menu, click **Modify Static Route**.
The Static Route dialog box appears.

3 Modify the static route attributes.

4 Click the **Save** button.

To delete a static route:

1 Click the static route you want to delete in the Static Route table.

2 On the **Configuration** menu, click **Delete Static Route**.
A confirmation message appears.

3 Click the **Yes** button.

IPX Routing

Business Communications Manager supports RIP and SAP (Service Advertising Protocol) for IPX routing in a NetWare environment. Static routes and static services are also supported.

Business Communications Manager supports IPX basic packet filtering feature.

This section provides instructions about how to configure IPX routing for specific interfaces. All available interfaces appear under the IPX Routing heading. The same configuration procedures apply to all interfaces.

Note: The IPX router manager in your Business Communications Manager system operates separately from the IP routing manager. As a result, RIP configuration under the IP Routing heading has no effect on IPX routing. You must configure IPX RIP parameters under the IPX Routing heading.

Tips
After you create and add a filter for IPX routing on an interface, you must select the Input Filter Action and Output filter Action from the RIP Summary parameters.

Warning: The filter action that indicates either to deny or allow packets that match filter definition applies to all filters. You cannot set a filter action for a specific filter. When you have decided which action the routing manager must perform on packets matching a filter definition, the routing manager performs this action every time it finds a match between packets and filters.

Enabling IPX Routing

IPX Routing does not appear on Unified Manager until you enable it.

To enable IPX Routing:

1. Launch your web browser.
2. In the URL address field, type the Business Communications Manager IP address, including the port number 6800.
   For example: *HTTP://10.10.10.1:6800*

   Note: You must include **HTTP://** with the address and port number to access Unified Manager when you are using Internet Explorer as your browser.

   The Business Communications Manager Unified Manager initial page appears.

3 Click the **Maintenance** button.
The Network Password screen appears.

4 In the **User Name** box, type the system administrator user name.
The default system administrator user name is *supervisor.*

5 In the **Password** box, type the system administrator password.
The default system administrator password is *visor.*

6 Click the **OK** button.
The Product Maintenance & Support screen appears.

7 Click the **Install Optional Components** link.
The Install Optional Components screen appears.

8 Click the **IPX Routing** link.
The IPX Routing install wizard starts.

9 Follow the prompts on the screen to enable IPX Routing.

The IPX Routing install wizard consists of three steps. Business Communications Manager reboots after each step.
It takes 10 to 15 minutes to enable IPX Routing.

Configuring IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** heading.
The IPX Routing Summary screen appears.

2 Configure the IPX Routing Summary settings. These settings are described in the following table.

Attribute	Description
Description	Displays the name of the router.
Version	Displays the version number of the router.
Status	Displays the current status of the service.
Internal Network Number	Allows you to specify the internal network number. The internal network number uniquely identifies the computer on the intranet.

3 Click the **IPX Global Settings** tab.
The IPX Global Settings screen appears.

4 Configure the IPX Global Settings. These setting are described in the following table.

Attribute	Description
IPX Log level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.

5 Click the **RIP Global Settings** tab.
The RIP Global Settings screen appears.

6 Configure the RIP Global Settings. These settings are described in the following table.

Attribute	Description
RIP Log level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.

7 Click the **SAP Global Settings** tab.
The SAP Global Settings screen appears.

8 Configure the SAP Global Settings. These settings are described in the following table.

Attribute	Description
SAP Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.

9 Press the **Tab** key to save the settings.

Configuring Packet Filters for IPX routing

Note: The maximum number of IPX filters you can add is 128.

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to configure for IPX routing.
   The Interface Summary screen appears.
3. Configure the IPX routing packet filter summary settings. These settings are described in the following table.

Attribute	Description
Interface Name	Displays the name of the interface you are currently configuring for IPX routing.
Input Filter Action	Allows you to specify the action the packet filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for filters. **Permit** all inbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "RIP filters for IPX routing" on page 390.
Output Filter Action	Allows you to specify the action the packet filter must perform on outbound traffic. The values possible values are: **Deny** all outbound traffic matching the criterion defined for filters. **Permit** all outbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can choose Permit. To create a filter, refer to "RIP filters for IPX routing" on page 390.
Network Number	Allows you to specify the network number (also called external network number) for routing purposes.
Frame Type	Allows you to specify the frame type. The possible values are: Ethernet II, Ethernet 802.2, Ethernet 802.3, Ethernet SNAP, Default.

4. Press the **Tab** key to save the settings.

Adding Packet Input filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to configure.
   The Interface Summary screen appears.
3. Click the **Packet Input Filters** tab.
   The Packet Input Filters screen appears.

4 On the **Configuration** menu, click **Add Packet Input Filter**.
The Packet Input Filters screen appears.

5 Configure the Packet Input Filter parameters. These parameters are described in the following table.

Attribute	Description
Packet Input Filter (PIF#)	Allows you to assign a number to the Packet Input Filter. For example, the valid packet input filter number for the first input filter is PIF1. The function of the Packet Input Filter number is to uniquely identify a packet input filter. If you add more than one Packet Input Filter, use sequential numbers. If you use the number of an existing Packet Input Filter, the system modifies the existing Packet Input Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Packet Input Filter, you cannot change the Packet Input Filter number.
Source Network Number	Allows you to enter the network number that identifies the source IPX network. A valid entry is any 4-byte hexadecimal number.
Source Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.
Source Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Source Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Destination Network Number	Allows you to enter the network number that identifies the destination IPX network. A valid entry is any 4-byte hexadecimal number.
Destination Network Mask	Allows you to enter the network mask to be applied to the destination address. This parameter defines the range of network numbers that you want to filter.

6 Click the **Save** button.

Modifying Packet Input filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **Packet Input Filters** tab.
The Packet Input Filters screen appears.

4 Click the Packet Input Filter you want to modify.

5 On the **Configuration** menu, click **Modify Packet Input Filter**.
The Packet Input Filters screen appears.

6 Modify the Packet Input Filter attributes.

7 Click the **Save** button.

Deleting Packet Input filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **Packet Input Filters** tab.
   The Packet Input Filters screen appears.
4. Click the Packet Input Filter you want to delete.
5. On the **Configuration** menu, click **Delete Packet Input Filter**.
   A confirmation message appears.
6. Click the **Yes** button.

Adding Packet Output filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **Packet Output Filters** tab.
   The Packet Output Filters screen appears.
4. On the **Configuration** menu, click **Add Packet Output Filter**.
   The Packet Output Filters screen appears.
5. Configure the Packet Output Filter parameters. These parameters are described in the following table.

Attribute	Description
Packet Output Filter (POF#)	Allows you to assign a number to the Packet Output Filter. For example, the valid Packet Output Filter number for the first output filter is POF1. The function of the Packet Output Filter number is to uniquely identify a Packet Output Filter. If you add more than one Packet Output Filter, use sequential numbers. If you use the number of an existing Packet Output Filter, the system modifies the existing Packet Output Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Packet Output Filter, you cannot change the Packet Output Filter number.
Source Network Number	Allows you to enter the network number that identifies the source IPX network. A valid entry is any 4-byte hexadecimal number.
Source Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.
Source Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Source Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Destination Network Number	Allows you to enter the network number that identifies the destination IPX network. A valid entry is any 4-byte hexadecimal number.
Destination Network Mask	Allows you to enter the network mask to be applied to the destination address. This parameter defines the range of network numbers that you want to filter.

6 Click the **Save** button.

Modifying Packet Output filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **Packet Output Filters** tab.
The Packet Output Filters screen appears.

4 Click the Packet Output Filter you want to modify.

5 On the **Configuration** menu, click **Modify Packet Output Filter**.
The Packet Output Filters screen appears.

6 Modify the Packet Output Filter attributes.

7 Click the **Save** button.

Deleting Packet Output filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **Packet Output Filters** tab.
The Packet Output Filters screen appears.

4 Click the Packet Output Filter you want to delete.

5 On the **Configuration** menu, click **Delete Packet Output Filter**.
A confirmation message appears.

6 Click the **Yes** button.

RIP filters for IPX routing

RIP is the routing protocol that routes IPX data packets in an internetwork environment. You can configure IPX packet filters for inbound or outbound traffic on interface handling IPX packets.

Note: The maximum number of IPX filters you can add is 128.

Configuring RIP for IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **RIP Summary** tab.
The RIP Summary screen appears.

4 Configure the RIP Summary settings. These settings are described in the following table.

Attribute	Description
Input Filter Action	Allows you to specify the action the packet filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for filters. **Permit** all inbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "RIP filters for IPX routing" on page 390.
Output Filter Action	Allows you to specify the action the packet filter must perform on outbound traffic. The values possible values are: **Deny** all outbound traffic matching the criterion defined for filters. **Permit** all outbound traffic matching the criterion defined for filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "RIP filters for IPX routing" on page 390.

5 Press the **Tab** key to save the settings.

6 Click the **RIP Parameters** tab.
The RIP Parameters screen appears.

7 Configure the RIP Parameters settings. These settings are described in the following table.

Attribute	Description
RIP State	Allows you to enable or disable RIP for this interface. The values are **Enabled** or **Disabled**. The default value is **Enabled**
Advertise Routes	Allows you enable or disable the advertisement of routes on the interface you are configuring. The default value is **Enabled**.
Accept Route Advertisements	Allows you to enable or disable the acceptance of route advertisement from remote routers on this interface. The default value is **Enabled**.
Update Mode	Allows you to select an update mode for the routing table. The routing table update modes available are: **Standard** update mode sends out a routing table for a router at regular intervals that you specify in the Update Interval box. New routes are added to the routing table as dynamic routes and are deleted from the routing tables when the router restarts. **Autostatic** update mode sends a routing table on the current interface when other routers connected to this interface request it. New routes to this interface, using RIP, are stored as static routes in the routing table for this interface and remain until you delete them. No Update mode never updates the routing tables on the current interface. The default value is **Standard**.

Attribute	Description
Update Interval	Allows you to set the interval, in seconds, when the routing manager updates the route tables. When you set the Update Mode to **Standard,** the routing manager periodically updates the route tables at the interval you specify in the Update Interval box. The possible values are 5 to 86400 seconds (24 hours). The default value is 60 seconds.
Aging Interval Multiplier	A multiplier used to determine when a route expires and is removed from the route table. For example, if the update interval is set to 60 seconds and you enter a value of 3 in the Aging Interval Multiplier, a route remains in the route table for a maximum of 180 seconds (3 X 60) from the last update. The default value is 3.

8 Press the **Tab** key to save the settings.

Adding RIP Input Filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **RIP Input Filters** tab.
The RIP Input Filters screen appears.

4 On the **Configuration** menu, click **Add RIP Input Filter**.
The RIP Input Filters screen appears.

5 Configure the RIP Input Filter parameters. These parameters are described in the following table.

Attribute	Description
Input Filter (IF#)	Allows you to assign a number to the RIP Input Filter. For example, the valid RIP input filter number for the first input filter is IF1. The function of the RIP Input Filter number is to uniquely identify a RIP input filter. If you add more than one RIP Input Filter, use sequential numbers. If you use the number of an existing RIP Input Filter, the system modifies the existing RIP Input Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a RIP Input Filter, you cannot change the RIP Input Filter number.
Network Number	Allows you to enter the network number that identifies the IPX network. A valid entry is any 4-byte hexadecimal number.
Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.

6 Click the **Save** button.

Modifying RIP Input filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Input Filters** tab.
   The RIP Input Filters screen appears.
4. Click the RIP Input Filter you want to modify.
5. On the **Configuration** menu, click **Modify RIP Input Filter**.
   The RIP Input Filters screen appears.
6. Modify the RIP Input Filter attributes.
7. Click the **Save** button.

Deleting RIP Input filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Input Filters** tab.
   The RIP Input Filters screen appears.
4. Click the RIP Input Filter you want to delete.
5. On the **Configuration** menu, click **Delete RIP Input Filter**.
   A confirmation message appears.
6. Click the **Yes** button.

Adding RIP Output filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **RIP Output Filters** tab.
   The RIP Output Filters screen appears.
4. On the **Configuration** menu, click **Add RIP Output Filter**.
   The RIP Output Filters screen appears.

5 Configure the RIP Output Filter parameters. These parameters are described in the following table.

Attribute	Description
Output Filter (OF#)	Allows you to assign a number to the RIP Output Filter. For example, the valid RIP Output Filter number for the first output filter is OF1. The function of the RIP Output Filter number is to uniquely identify a RIP Output Filter. If you add more than one RIP Output Filter, use sequential numbers. If you use the number of an existing RIP Output Filter, the system modifies the existing RIP Output Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a RIP Output Filter, you cannot change the RIP Output Filter number.
Network Number	Allows you to enter the network number that identifies the IPX network. A valid entry is any 4-byte hexadecimal number.
Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.

6 Click the **Save** button.

Modifying RIP Output filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **RIP Output Filters** tab.
The RIP Output Filters screen appears.

4 Click the RIP Output Filter you want to modify.

5 On the **Configuration** menu, click **Modify RIP Output Filter**.
The RIP Output Filters screen appears.

6 Modify the RIP Output Filter attributes.

7 Click the **Save** button.

Deleting RIP Output filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **RIP Output Filters** tab.
The RIP Output Filters screen appears.

4 Click the RIP Output Filter you want to delete.

5 On the **Configuration** menu, click **Delete RIP Output Filter**.
A confirmation message appears.

6 Click the **Yes** button.

SAP filters for IPX routing

On a Novell network, the Service Advertising Protocol (SAP) provides network control information about available services on a Novell network. You can define and add SAP filters for IPX routing.

Note: The maximum number of IPX filters you can add is 128.

Configuring the SAP for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **SAP Summary** tab.
   The SAP Summary screen appears.
4. Configure the SAP Summary settings. These settings are described in the following table.

Attribute	Description
Input Filter Action	Allows you to specify the action the filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for SAP filters. **Permit** all inbound traffic matching the criterion defined for SAP filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "SAP filters for IPX routing" on page 395.
Output Filter Action	Allows you to specify the action the filter must perform on outbound traffic. The possible values are: **Deny** all outbound traffic matching the criterion defined for SAP filters. **Permit** all outbound traffic matching the criterion defined for SAP filters. The default value is **Deny**. **Note**: You must create a filter before you can assign an action. To create a filter, refer to "SAP filters for IPX routing" on page 395.

5. Press the **Tab** key to save the settings.
6. Click the **SAP Parameters** tab.
   The SAP Parameters screen appears.
7. Configure the SAP Parameters. These parameters are described in the following table.

Attribute	Description
SAP State	Allows you to enable or disable SAP for this interface. The possible values are **Enabled** or **Disabled**. The default value is **Enabled**.

Attribute	Description
Advertise Services	Allows you to enable or disable the advertisement of SAP services on the interface to remote routers. The possible values are **Enabled** or **Disabled**. The default value is **Enabled**.
Accept Service Advertisements	Allows you to enable or disable the acceptance of advertisement of SAP services from remote routers. The possible values are **Enabled** or **Disabled**. The default value is **Enabled.**
Update Mode	Allows you to select an update mode for SAP on the interface. The available options are: **Standard** update mode sends periodic updates at an interval you define in the Update Interval box. **Autostatic** update mode sends a routing table update when other routers connected to this interface request it. New routes to this interface, using SAP, are stored as static routes in the routing table for this interface and remain until you delete them. **No Update** mode never updates the routing tables on the current interface. The default value is **Standard**.
Update Interval	Allows you to set the interval, in seconds at which SAP announcements are updated. If you set the **Update Mode** to **Standard**, the SAP announcements are updated at the interval you specify in the Update Interval box. The possible values **5** to **86400** seconds. The default value is **60** seconds.
Aging Interval Multiplier	A multiplier used to determine when a SAP announcements coming to this interface expires. For example, if the update interval is set to 60 seconds and you enter a value of 3 in the Aging Interval Multiplier, a SAP announcement remains valid for a maximum of 180 seconds (3 X 60) from the last announcement. The possible values are **3** to **100**. The default value is **3**.

Adding SAP Input Filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **SAP Input Filters** tab.
   The SAP Input Filters screen appears.
4. On the **Configuration** menu, click **Add SAP Input Filter**.
   The SAP Input Filters screen appears.

5 Configure the SAP Input Filter parameters. These parameters are described in the following table.

Attribute	Description
Input Filter (SapIF#)	Allows you to assign a number to the SAP Input Filter. For example, the valid SAP input filter number for the first input filter is SapIF1. The function of the SAP Input Filter number is to uniquely identify a SAP input filter. If you add more than one SAP Input Filter, use sequential numbers. If you use the number of an existing SAP Input Filter, the system modifies the existing SAP Input Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a SAP Input Filter, you cannot change the SAP Input Filter number.
Service Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Service Name	Allows you to enter the service name. You can use a wildcard service name such as "*" to indicate all service names.

6 Click the **Save** button.

Modifying SAP Input Filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **SAP Input Filters** tab.
The SAP Input Filters screen appears.

4 Click the SAP Input Filter you want to modify.

5 On the **Configuration** menu, click **Modify SAP Input Filter**.
The SAP Input Filters screen appears.

6 Modify the SAP Input Filter attributes.

7 Click the **Save** button.

Deleting SAP Input Filters

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface you want to modify.
The Interface Summary screen appears.

3 Click the **SAP Input Filters** tab.
The SAP Input Filters screen appears.

4 Click the SAP Input Filter you want to delete.

5 On the **Configuration** menu, click **Delete SAP Input Filter**.
A confirmation message appears.

6 Click the **Yes** button.

Adding SAP Output Filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **SAP Output Filters** tab.
   The SAP Output Filters screen appears.
4. On the **Configuration** menu, click **Add SAP Output Filter**.
5. Configure the SAP Output Filter parameters. These parameters are described in the following table.

Attribute	Description
Output Filter (SapOF#)	Allows you to assign a number to the SAP Output Filter. For example, the valid SAP output filter number for the first output filter is SapOF1. The function of the SAP Output Filter number is to uniquely identify a SAP Output filter. If you add more than one SAP Output Filter, use sequential numbers. If you use the number of an existing SAP Output Filter, the system modifies the existing SAP Output Filter. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a SAP Output Filter, you cannot change the SAP Output Filter number.
Service Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Service Name	Allows you to enter the service name. You can use a wildcard service name such as "*" to indicate all service names.

6. Click the **Save** button.

Modifying SAP Output Filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.
3. Click the **SAP Output Filters** tab.
   The SAP Output Filters screen appears.
4. Click the SAP Output Filter you want to modify.
5. On the **Configuration** menu, click **Modify SAP Output Filter**.
6. Modify the SAP Output filter attributes.
7. Click the **Save** button.

Deleting SAP Output Filters

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface you want to modify.
   The Interface Summary screen appears.

3 Click the **SAP Output Filters** tab.
The SAP Output Filters screen appears.

4 Click the SAP Output Filter you want to delete.

5 On the **Configuration** menu, click **Delete SAP Output Filter**.
A confirmation message appears.

6 Click the **Yes** button.

Static Routes for IPX Routing

You can add static routes to the IPX routing table. The IPX static routes take precedence over the routes added by routing protocol such as RIP.

Note: The maximum number of IPX routes you can add is 128.

Adding Static Routes for IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface that you want to configure.

3 Click the **Static Routes** tab.
The Static Routes screen appears.

4 On the **Configuration** menu, choose **Add Static Route**.
The Static Routes dialog box appears.

5 Configure the static routing table attributes. These attributes are described in the following table.

Attribute	Description
Static Route (SR#)	Allows you to assign a number to the Static Route. For example, the valid Static Route number for the first static route is SR1. The function of the Static Route number is to uniquely identify a Static Route. If you add more than one Static Route, use sequential numbers. If you use the number of an existing Static Route, the system modifies the existing Static Route. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Static Route, you cannot change the Static Route number.
Net Number	IPX Network Number identifies the destination network for the routing table entry. The permitted value is 4 bytes in hexadecimal format. The default value is **None**.
Next Hop Mac Address	Shows the MAC address of the next hop router to reach the network defined in the **NetNumber** box. The permitted value is 6 bytes in hexadecimal format. The default value is **None**.
Ticks	Time required (in 1/60 seconds) to reach the destination network. The values are **1** to **32,767**. The default value is **None**.
Hops	Shows the number of hops that must be crossed in order to reach the destination network. The permitted values are **0** to **15**. The default value is **0**.

6 Click the **Save** button.

Modifying Static Routes for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface that you want to configure.
3. Click the **Static Routes** tab.
   The Static Routes screen appears.
4. Click the Static Route you want to modify.
5. On the **Configuration** menu, choose **Modify Static Route**.
   The Static Routes dialog box appears.
6. Modify the static routing table attributes.
7. Click the **Save** button.

Deleting Static Routes for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface that you want to configure.
3. Click the **Static Routes** tab.
   The Static Routes screen appears.
4. Click the Static Route you want to delete.
5. On the **Configuration** menu, choose **Delete Static Route**.
   A confirmation message appears.
6. Click the **Yes** button.

Static Service for IPX Routing

Adding a Static Service for IPX Routing

1. On the navigation tree, click the **Services** key and click the **IPX Routing** key.
2. Click the interface that you want to configure.
3. Click the **Static Services** tab.
   The Static Service screen appears.
4. On the **Configuration** menu, choose **Add Static Service**.
   The Static Routes dialog box appears.

5 Configure the static service attributes These attributes are described in the following table.

Attribute	Description
Static Service (SS#)	Allows you to assign a number to the Static Service. For example, the valid Static Service number for the first Static Service is SS1. The function of the Static Service number is to uniquely identify a Static Service. If you add more than one Static Service, use sequential numbers. If you use the number of an existing Static Service, the system modifies the existing Static Service. If you use non-sequential, numbers the system automatically reassigns sequential numbers. When you modify a Static Service, you cannot change the Static Service number.
Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Name	Shows the static service name. The permitted values can use up to 48 bytes. A wildcard character (*) can also be selected to indicate all service names.
Network	Shows the network part of the service address. The permitted value uses 4 bytes in hexadecimal format. The default value is **None**.
Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Hops	Shows the number of hops to reach the destination network. The permitted values are **0** to **15**. The default value is **0**.

6 Click the **Save** button to save your settings.

Modifying a Static Service for IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface that you want to configure.

3 Click the **Static Services** tab.
The Static Service screen appears.

4 Click the Static Service you want to modify.

5 On the **Configuration** menu, choose **Modify Static Service**.
The Static Routes dialog box appears.

6 Modify the static service attributes.

7 Click the **Save** button to save your settings.

Deleting a Static Service for IPX Routing

1 On the navigation tree, click the **Services** key and click the **IPX Routing** key.

2 Click the interface that you want to configure.

3 Click the **Static Services** tab.
The Static Service screen appears.

4. Click the Static Service you want to delete.
5. On the **Configuration** menu, choose **Delete Static Service**.
   A confirmation message appears.
6. Click the **Yes** button.

SNMP

The SNMP service in Business Communications Manager responds to requests from management stations, generates SNMP traps corresponding to events and reports to trap subscriber stations.

Guidelines for using SNMP

Consider the following guidelines when using SNMP:

- You can set read-only and read-write community names.
- You can set a list of permitted managers. When set, the agent responds to SNMP managers requests from those IP hosts only.
- An empty list of permitted managers implies that the agent responds to requests from anyone.
- You can set trap communities. Each trap entry identifies the community name that must be used and the manager addresses.
- You can enable or disable sending authentication traps.
- You can enable or disable the SNMP agent.

Note: You can use the Alarm Manager to enable or disable the sending of all or some types of SNMP traps. For more information about Alarm Manager, refer to "Alarm Manager" on page 481.

Configuring SNMP

1. On the navigation tree, click the **Services** key, and click the **SNMP** heading.
   The SNMP Summary screen appears.
2. Configure the SNMP summary attributes. These attributes are described in the following table.

Attribute	Description
Description	Shows the description of the SNMP agent.
Version	Shows the version of the SNMP agent.
Status	Allows you to enable or disable the SNMP agent.
Authentication Failure Traps	Allows you to disable authentication failure traps. When enabled, the SNMP agent sends authentication failure traps if there is an authentication failure. Authentication failure happens if an SNMP manager application provides a wrong community string or performs an operation that is not permitted for a community.

SNMP Community List

To modify the Community List, use the following procedures.

Adding a community to the list

1. On the navigation tree, click the **Services** key, and click the **SNMP** heading.
   The SNMP Summary screen appears.
2. Click the **Community List** tab.
   The Community List screen appears.
3. On the **Configuration** menu, click **Add Community**.
   The Community List dialog box appears.
4. Configure the Community List attributes. These attributes are described in the following table.

Attribute	Description
Community List (C#)	Allows you to specify the entry name used as a key to uniquely identify an individual community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix C followed by a unique number that identifies the community name entry on the agent. For example, C2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing community entry name, it modifies the existing community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a community entry, you can't change the name. The community entry name does not have any significance other than to identify an entry.
Community Name	Allows you to specify the name of the community that the individual managers use to interact with this agent. The name is case sensitive. The default community names are **public** and **Private**. If there are no community names listed, then all community names are accepted. All the community names are global to the agent. In other words, you cannot associate a specific community name with a single management station.
Access Permission	Allows you to specify the read and write access for this community. The following options are available: **READ-ONLY** and **READ-WRITE** The default value is **READ-ONLY**.

5. Click the **Save** button.

Modifying a community

1. On the navigation tree, click the **Services** key, and click the **SNMP** heading.
   The SNMP Summary screen appears.
2. Click the **Community List** tab.
   The Community List screen appears.
3. Click the community you want to modify.
4. On the **Configuration** menu, click **Modify Community**.
   The Community List dialog box appears.

5 Modify the Community attributes.

6 Click the **Save** button.

Deleting a community

1 On the navigation tree, click the **Services** key, and click the **SNMP** heading.
The SNMP Summary screen appears.

2 Click the **Community List** tab.
The Community List screen appears.

3 Click the community you want to delete.

4 On the **Configuration** menu, click **Delete Community**.
A message appears that asks you to confirm the deletion.

5 Click the **Yes** button.

Manager List

To modify the Manager List, use the following procedures.

Adding a manager to the Manager List

1 On the navigation tree, click the **Services** key, and click the **SNMP** heading.
The SNMP Summary screen appears.

2 Click the **Manager List** tab.
The Manager List screen appears.

3 On the **Configuration** menu, click **Add Manager**.
The Manager List dialog box appears.

4 Configure the Manager List attributes. These attributes are described in the following table.

Attribute	Description
Manager List (M#)	Allows you to specify the entry name used to identify an individual manager entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix M followed by a unique number that identifies the manager entry on the agent. For example, M2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing manager entry name, it modifies the existing manager entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a manager entry, you cannot change the name. The manager entry name uniquely identifies an entry.
Manager IP Address	Allows you to specify the IP Address of the SNMP Manager station corresponding to this entry. If no manager entries are created, the Business Communications Manager device accepts SNMP requests from all stations. If there is a list of manager entries, Business Communications Manager server accepts SNMP requests from the IP Addresses specified in the list.

5 Click the **Save** button.

Modifying a manager

1. On the navigation tree, click the **Services** key, and click the **SNMP** heading.
   The SNMP Summary screen appears.
2. Click the **Manager List** tab.
   The Manager List screen appears.
3. Click the manager you want to modify.
4. On the **Configuration** menu, click **Modify Manager**.
   The Manager List dialog screen appears.
5. Modify the manager attributes.
6. Click the **Save** button.

Deleting a manager

1. On the navigation tree, click the **Services** key, and click the **SNMP** heading.
   The SNMP Summary screen appears.
2. Click the **Manager List** tab.
   The Manager List screen appears.
3. Click the manager you want to delete.
4. On the **Configuration** menu, click **Delete Manager**.
   A message appears that asks you to confirm the deletion.
5. Click the **Yes** button.

Trap Community List

To modify the Trap Community List, use the following procedures.

Adding a trap community to the Trap Community List

1. On the navigation tree, click the **Services** key, and click the **SNMP** heading.
   The SNMP Summary screen appears.
2. Click the **Trap Community List** tab.
   The Trap Community List screen appears.
3. On the **Configuration** menu, click **Add Trap Community**.
   The Trap Community List screen appears.

4 Configure the Trap List attributes. These attributes are described in the following table.

Attribute	Description
Trap List (T#)	Allows you to specify the entry name used to identify an individual trap community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix T followed by a unique number that identifies the trap community entry on the agent. For example, T2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing trap community entry name, it modifies the existing trap community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a trap community entry, you can't change the name. The trap community entry name does not have any significance, other than to uniquely identify an entry.
Community Name	The community name is case sensitive and encoded in each trap message. This name can not be in the Community List.
Manager IP Address	Allows you to specify the IP addresses of the SNMP trap subscriber stations. If you have too many IP addresses in the trap community list, the SNMP service may degrade system performance.

5 Click the **Save** button.

Modifying a trap community

1 On the navigation tree, click the **Services** key, and click the **SNMP** heading.
The SNMP Summary screen appears.

2 Click the **Trap Community List** tab.
The Trap Community List screen appears.

3 Click the trap community you want to modify.

4 On the **Configuration** menu, click **Modify Trap Community**.
The Trap Community List dialog box appears.

5 Modify the trap community attributes.

6 Click the **Save** button.

Deleting a trap community

1 On the navigation tree, click the **Services** key, and click the **SNMP** heading.
The SNMP Summary screen appears.

2 Click the **Trap Community List** tab.
The Trap Community List screen appears.

3 Click the trap community you want to delete.

4 On **Configuration** menu, click **Delete Trap Community**.
A message appears that asks you to confirm the deletion.

5 Click the **Yes** button.

QoS monitor

The IP telephony Quality-of-Service (QoS) Monitor periodically monitors the delay and jitter of IP networks between two peer gateways. The Business Communications Manager QoS Monitor uses the same method as the Meridian 1 ITG. These monitoring packets are delivered at UDP port 5000.

QoS Monitor works on a gateway between two Business Communications Manager systems or between a Business Communications Manager system and a Meridian 1 ITG system. QoS Monitor must be enabled on both ends of the connection.

For information about how to configure remote gateways, refer to the *Business Communications Manager IP Telephony Configuration Guide*.

Note: The remote gateways are identified by their Published IP Addresses. If a remote gateway is accessed through an interface with Network Address Translation (NAT) configured, the Published IP Address must be the same as one of the Public IP Addresses. For information about NAT, refer to "NAT (Network Address Translation)" on page 416.

The main objective of the QoS Monitor is to allow new IP telephony calls to fall back to the PSTN if the IP network is detected as "bad".

To set the QoS monitor:

1. On the navigation tree, click the **Services** key and click the **QoS Monitor** heading. The QoS Monitor Summary screen appears.
2. Configure the QoS Monitor Summary attributes. These attributes are described in the following table.

Attribute	Description
Description	Shows the description of the service.
Status	Allows you to enable or disable the service.
Version	Shows the version of the service.

3. Press the **Tab** key to save the settings.

QoS Monitor Mean Opinion Score

To view the QoS Monitor Mean Opinion Score:

1. On the navigation tree, click the **Services** key and click the **Qos Monitor** key.
2. Click the **Mean Opinion Score** heading.

If you configure or create remote gateways, the mean opinion scores of the connections to these remote gateways are displayed in the screen. The mean opinion scores are a measure of the quality of the voice link, while using an IP trunk, for each codec type. Each configured gateway appears on a separate row.

Each row consists of the fields for the name of the remote gateway, its IP address, the status of the QoS monitoring for the connection, and the mean opinion scores for each allowed voice codec type and for each direction.

If the QoS Monitor setting for the remote gateway entry is Disabled, the MOS values for the remote gateway appear as N/A. If the QoS Monitor service is disabled or down for any reason, all MOS values appear as N/A. Also, if no MOS reports are received from a remote gateway, the MOS values in the Received (Recv) direction appear as N/A.

The MOS values are updated inside the QoS Monitor service every 15 seconds. These updates are a running average of the last five sampled values, which span approximately 75 seconds.

The MOS values that appear are updated automatically. To display the current MOS values, on the **View** menu, click **Refresh**.

Web cache

When you use Business Communications Manager as a web proxy, Business Communications Manager can store, or cache, information downloaded from the Internet. A proxy is a server that acts on behalf of another. Web caching allows LAN workstations to share common information downloaded from the Internet.

With Business Communications Manager configured as a web proxy with web caching:

- LAN workstations have shorter download times.
- The system stores previously downloaded information for future use by all workstations on the LAN.
- Business Communications Manager retrieves information from the Internet only if it is not already cached or if the cached file is out of date compared to the information on the Internet.

You can also configure the web caching settings on your computer through your web browser.

The web proxy also provides security features similar to the DNS proxy. It hides all of the internal browsers' IP addresses from external web servers. External web servers see only the Business Communications Manager IP address.

Guidelines for using Web Caching/Proxy

The Business Communications Manager web proxy uses a web server for running in HTTP-Proxy mode.

Consider the following guidelines when using web caching/proxy:

- You cannot use the web server installed on Business Communications Manager as a general purpose HTTP server. It is only used by the Business Communications Manager web-based management client and web-cache services.
- If you want to run web sites on your network, you must have a separate HTTP server running on a system other than the Business Communications Manager system. There are two options available for the IP address you publish for your website.You can publish a separate IP address for the HTTP server or you can publish the same IP address as your Business Communications Manager.
  To publish a separate IP address for the HTTP server, publish the IP address of the computer on which you are running the HTTP server.
  To publish the same IP address used for Business Communications Manager, set up a NAT rule to change the public address of the HTTP server to the IP address of Business Communications Manager.
- Some secure web sites are not accessible through the Business Communications Manager web cache service. If you are having problems accessing a secure web site, turn off the web cache service and try again.
- Web cache is enabled by default.

To configure the web cache settings:

1. On the navigation tree, click the **Services** key and click the **Web Cache** heading. The Web Cache Summary screen appears.
2. Configure the Web Cache attributes. These attributes are described in the following table.

Attribute	Description
Description	Shows the description of the Web Cache server.
Version	Shows the version of the Web Cache server.
Status	Shows the status of the Web Cache server. This setting is read-only. The Web Cache server always runs to provide support for Unified Manager.
Server Address	Allows you to specify which IP address to use for interacting with HTTP clients. Since Business Communications Manager typically has more than one IP interface and associated IP Address, users can choose this value. The default for this value is the IP address of the first LAN interface. This value changes when the IP address of the first LAN interface changes. Exercise caution if modifying this value.
Cache Mode	Allows you to enable or disable the cache-mode. The default value is **Enabled**.
Cache Size	Allows you to specify the maximum size (1 - 100,000), in KB, of the cache. The default value is **20480** KB.
Garbage Collection Interval	Allows you to specify the interval, in hours, between garbage collection operations on the cache. The values are **1** to **24**. The default value is **4** hours.
Cache Maximum Life	Allows you to specify the maximum life, in hours, on the proxy server for cached HTTP pages. Values are **1** to **24**. The default value is **24** hours.
Maximum Server Threads	Allows you to specify the number of threads ready to serve HTTP requests in the proxy server. Values are **1** to **255**. The default value is **16** threads.

3. Press the **Tab** key to save the settings.

Net Link Manager

Net Link Manager is a Business Communications Manager service that provides constant primary link status monitoring. Net Link Manager is also where you select your WAN primary and backup interfaces.

When Net Link Manager detects a primary WAN link failure, Net Link Manager automatically establishes a backup WAN connection, if one is configured. Net Link Manager monitors the WAN primary link by performing multiple tests. When a predetermined number of tests fails, Net Link Manager establishes the backup connection.

The backup connection uses a V.90 modem (North America) or one or more ISDN B channels. When the backup WAN connection is active, Net Link Manager continues to monitor the status of the primary WAN link connection. When the primary WAN link connection is determined to be available again, Net Link Manager re-establishes the primary WAN link and disconnects the backup connection.

Warning: If an ISDN dial-up connection is used as the primary WAN connection, no backup link is available.

Note: Net Link Manager manages the default route in Business Communications Manager. If the primary link fails, Net Link Manager removes the default route from the Primary link and adds it to the backup link. This happens during the switch over from primary to backup link. The default route returns to the primary link after the connection to the primary WAN link is re-established.

Note: Net Link Manager manages the default route in Business Communications Manager. If a link breaks, Net Link Manager removes all the default routes on the broken link and adds them to the backup link. This happens during switch over from primary to secondary link. The default routes return to the primary link after the connection to the primary WAN link is reestablished.

To enable or disable Net Link Manager:

1 On the navigation tree, click the **Services** key and click the **Net Link Mgr** heading. The Net Link Manager Summary screen appears.

2 Configure the Net Link Manager attributes. These attributes are described in the following table.

Attribute	Description
Description	Shows a description of Net Link Manager.
Version	Shows the version number of the subsystem.
Status	Shows the status of Net Link Manager. This box also provides commands to enable or disable Net Link Manager. Possible values: **Up**, **Disabled**, **Enabled** The default value is: **Up**

3 Press the **Tab** key to save the settings.

Selecting a permanent WAN link as the primary WAN connection

1 On the navigation tree, click the **Services** key and click the **Net Link Mgr** heading.
The Net Link Manager Summary screen appears.

2 Click the **Primary WAN Connection** tab.
The Primary WAN Connection screen appears

3 Click the **Mode** box and click **Permanent.**

4 Press the **Tab** key to save your choice.

5 Click the **Permanent WAN Connection Setting** tab
The Permanent WAN Connection Setting screen appears.

6 Configure the Permanent WAN Connections Setting attributes. These attributes are described in the following table.

Next Hop on Primary Link	Allows you to enter the IP address (in dot format) of the next hop router. This address is used by Net Link Manager to add a default route in Business Communications Manager. If this address ever becomes unreachable, Net Link Manager dials the backup link and changes the default route. This is usually the remote router of the primary WAN link. For more information on setting up remote router, see Appendix A, “Setting Up Remote Routers for IP Telephony prioritization,” on page 555.
Up Poll Interval	Allows you to set the polling interval on the Primary WAN Link, in seconds. The up poll interval is the interval between successive pings when the next hop on the primary link is available.
Down Poll Interval	Allows you to set the polling interval on the Primary WAN Link, in seconds, when the primary WAN link is down, and the backup (dial-up) WAN link is operational. A short interval provides faster recovery.

Switch Over Delay	Allows you to define the interval, in seconds, that Net Link Manager waits before switching back to the primary WAN link when it becomes available. This delay is to let the router at the other end of the primary link recognize that the primary link has come up and allows for necessary routing table updates. The default value is **30** seconds.
Backup Dial-up Interface	Allows you to select which dial up interface to use for WAN backup. You must configure a backup interface before you can select it. When you are configuring the backup interface, make sure you include “backup” in the interface name. Only interfaces with “backup” in their name appear on this list. For information about how to create an ISDN backup interface, refer to “Creating an ISDN dial up interface” on page 341.

7 Press the **Tab** key to save the settings.

Selecting a dial-up link as the primary WAN connection

The dial-up WAN connection supports PPP only. Business Communications Manager supports ISDN dial-up WAN connection.

Setting a dial-up connection as the primary WAN connection means that the Business Communications Manager default route is to the dial-up connection. If the dial-up WAN connection is configured as dial-on-demand, any traffic across the dial-up WAN connection causes the link to be established. Also, if there is no traffic crossing the connection, the link shuts down automatically after a time out.

Note: When you configure your primary WAN connection to use a dial-up WAN connection, no backup WAN connection is available.

1 On the navigation tree, click the **Services** key and click the **Net Link Manager** heading.
The Net Link Manager Summary screen appears.

2 Click the **Primary WAN Connection** tab.
The Primary WAN Connection screen appears

3 Click the **Mode** box and click **Dialup**.

4 Press the **Tab** key to save your choice.

5 Click the **Primary WAN Connection Setting** tab.
The Primary WAN Connection Setting screen appears.

6 From the **Primary Dial-up Interface** box, click the dial-up interface you want to use.

Tips
Before you can select a dial-up interface to connect to the network, you must first create a dial-up interface under Resources, Dial up. For information on creating a dial-up interface, see “Dial Up” on page 338.

7 Press the **Tab** key to save the settings.

Alarm Service

Business Communications Manager Alarm Service performs the following functions:

- Monitors Windows NT event logs for incoming events.
- Synchronizes Windows NT logs with Business Communications Manager alarm database.
- Receives events (alarms) from other Business Communications Manager applications through its API and logs the events in the Business Communications Manager database.
- Archives alarm history based on the criteria defined in Alarm Manager.
- Monitors the alarm configuration changes and updates SNMP trap agent and Alarm Service.

To enable or disable Alarm Service settings:

1. On the navigation tree, click the **Services** key and click the **Alarm Service** heading.
   The Alarm Service Summary screen appears.
2. Click the **Status** box and click **Enable** or **Disable**.
   The default value is **Disable**.
3. Press the **Tab** key to save the settings.

Note: The Alarm Service is disabled by default. You must enable Alarm Service to view alarms on the Alarm Banner.

NAT (Network Address Translation)

Business Communications Manager provides security and firewall features to protect your private data resources from outsiders. The Network Address Translation feature is a network security feature. NAT is the translation of IP addresses used within your private network to different IP addresses known to Internet users outside your private network. NAT helps ensure network security because each outgoing or incoming request must go through a translation process that also provides the opportunity to qualify or authenticate the request or match it to a previous request. NAT also translates port numbers.

NAT is defined by creating a set of rules and then defining the order in which these rules are evaluated.

Business Communications Manager supports both static and dynamic NAT for a number of packet types and protocols:

NAT Support for:	Type
Packets (static and dynamic)	TCP, UDP, IP
Protocols	H.323, FTP, HTTP, POP3, Telnet, SMTP, DNS, TFTP, GOPHER, FINGER, NNTP, RPC, SUNNFS and SNMP

Static NAT

Static NAT is the one-to-one mapping of an IP address on your private network to an IP address from outside your network. Inbound rules must have external IP addresses mapped to specific internal IP addresses.

Dynamic NAT

Dynamic NAT is the mapping between a private network and the outside network, of one address to a pool of addresses, a pool of addresses to one address or a pool of addresses to another. The mappings are made in a translation table and remain there until the table is cleared or until an entry times out.

Note: When using an inbound translation, be sure that all private addresses belong to the existing systems.

NAT and IP Firewall filters

When you use NAT and IP Firewall filters, there are two interactions you need to be aware of.

- On inbound traffic, the NAT rules are applied before the IP Firewall Filter rules.
- On outbound traffic, the IP Firewall Filter rules are applied before theNAT rules.

Managing Business Communications Manager

You cannot manage a Business Communications Manager system through another Business Communications Manager system when it is on the Private side of a NAT enabled interface.

Enabling and disabling NAT

1 On the navigation tree, click the **Services** key and click the **NAT** heading.
The NAT Summary screen appears.

2 Configure the NAT Summary attributes. These attributes are described in the following table.

Attribute	Description
Description	Shows a description of NAT.
Version	Shows the version number of the subsystem.
Status	Allows you to enable or disable NAT. Possible values: **Disabled**, **Enabled** The default value is: **Disabled**

3 Press **Tab** to save the setting.

Note: Do not enabled NAT on systems that use Fast Routing between LANs. If you enable NAT and Fast Routing, the packets will not be routed correctly. For information about Fast Routing, refer to "Setting LAN global parameters" on page 320.

Configuring an Interface with NAT

1 On the navigation tree, click the **Services** key and click the **NAT** key.

2 Click the interface you want to configure. For example: **LAN1**.
The Rule Order screen appears.

Note: Rules can be configured in several ways, using default rules, setting up individual rules or a combination of the two.

Adding Default rules

3 Click the **Default Rules** box and click **Enabled** or **Disabled**.
If you choose Enabled, two default rules are set. One is for TCP/UDP and the other for IP. Both default rules are outbound. These rules allow all outbound traffic to pass and stop all inbound traffic. The IP address for the Public address is the IP address of the interface you configure. The system automatically fills in the rule order. If you choose to add additional rules, the default rules still remain.
If you choose Disabled, the Default Rules are removed.
The default is Disabled.

Note: The default rules are only for traffic initiated in the outbound direction. You must add rules for inbound traffic or packets will pass in without translation.

Note: Before you can specify the Rule Order you must first add the Rules.

4 Press the **Tab** key to save the settings.

Adding a Rule to an interface

The maximum number of Rules you can add is 32.

1 Click the **Rule Setting** tab.
The Rule Setting screen appears.

2 On the **Configuration** menu, click **Add Rule**.
The Rule Setting dialog box appears.

3 Configure the Rule settings according to the following table.

Attribute	Description
Rule Name (R#)	Allows you to assign a number to the Rule. The Rule Name uniquely identifies a Rule. The value for this setting must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the rule. For example, 'R2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing rule name, it modifies the existing rule. If you use nonsequential numbers, the system automatically reassigns sequential numbers. When you modify a rule, you cannot change the rule name. The rule name does not have any significance other than identifying an entry.
Direction	Allows you to choose the direction of the rule: **In**, **Out** or **Both**. **Both** applies only to IP protocols.
Protocol	Allows you to choose the protocol for this interface; **IP**, **TCP**, **UDP**, or **TCP/UDP**.
Private IP Type	Allows you to specify if the IP type is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Private IP and Private Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Private IP	Allows you to specify the Private IP address. If the Private IP type is fixed, the Rule is invalid without this IP address.
Private Mask	Allows you to specify the mask to use with the Private IP. If you want the Rule to apply to a single Private IP address (the Private IP entered), enter 255.255.255.255. If you want the Rule to apply to all Private IP addresses, enter 0.0.0.0.
Private Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following: **ALL**, **FTP**, **Telnet**, **SMTP**, **DNS**, **Finger**, **HTTP**, **H.323**, **POP3**, **NNTP**, **RPC**, **SUNNFS, SNMP, SNMP-TRAP, TFTP and Gopher**.

Attribute	Description
Public IP Type	Allows you to specify if the IP type is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Public IP and Public Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Public IP	Allows you to specify the Public IP address. This address should be on the outside network.
Public Mask	Allows you to specify the mask to use with the Public IP. If you want the Rule to apply to a single Public IP address (the Public IP entered), enter 255.255.255.255. If you want the Rule to apply to all Public IP addresses, enter 0.0.0.0.
Public Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following; **ALL**, **FTP**, **Telnet**, **SMTP**, **DNS**, **Finger, HTTP, H.323, POP3, NNTP, RPC, SUNNFS, SNMP, SNMP-TRAP, TFTP and Gopher**.

Note: If you do not configure the public and private masks correctly, mappings to non-existent systems can occur. You must specify addresses that exist. For example, if you configure an outbound rule, the Public IP address and Public Mask are the translated addresses. These addresses must be assigned or packets will be sent to a non-existent destination. For inbound rules, the translated address is the Private Address and Mask.

If you want the rule to apply to one IP address only, you must enter a Mask of 255.255.255.255. If you enter any other Mask, the rule will apply to more than one IP address.

4 Click the **Save** button.

Modifying a Rule to an Interface

1 Click the **Rule Setting** tab.
The Rule Setting screen appears.

2 Click the rule you want to modify.

3 On the **Configuration** menu, click **Modify Rule**.
The Rule Setting dialog box appears.

4 Modify the Rule settings.

5 Click the **Save** button.

Deleting a Rule to an Interface

1 Click the **Rule Setting** tab.
The Rule Setting screen appears.

2 Click the rule you want to delete.

3 On the **Configuration** menu, click **Delete Rule**.
A message appears that asks you to confirm the deletion.

4 Click the **Yes** button.

Configuring the Rule order

1 When you finish adding rules, click the **Rule Order** tab.
The Rule Order screen appears.

2 In the **Rule Order** box, configure the order of the rules.

Note: Configure the rule order from most specific to most general. For example, a TCP rule for one port should come before a general rule for all TCP traffic. IP rules should come last.

3 Press **Tab** to update the screen.

Examples of common NAT configurations

A Business Communications Manager has two LANs and a WAN. The WAN connects to the outside and has one public IP address. The LANs are part of a private network. The system maps all outgoing traffic. HTTP traffic is mapped to 10.10.10.4. LAN1 subnet is 10.10.10.0, LAN2 is 10.10.11.0. The WAN address is 48.123.35.41.

The rules would be as follows:

Rule: R4
Direction: In
Private IP Type: Fixed
Protocol: TCP
Private IP Address: 10.10.10.4
Private IP Mask: 255.255.255.255
Private Port Range: HTTP
Public IP type: Fixed
Public IP Address: 48.123.35.41
Public IP mask: 255.255.255.255
Public Port Range: 8080

Default Rules: Enabled Including IP Phones

Rule Order: R1,R2,R3,R4

Note: This setting for Default Rules adds three rules. Additional rules start at R4.
Note: Spaces are not allowed between rule numbers.

A Business Communications Manager has two LANs and a WAN. The WAN connects to an Internet Service Provider that assigns the IP address. The LANs are part of a private network. The system maps all outgoing traffic. HTTP traffic is mapped to 10.10.10.4. LAN1 subnet is 10.10.10.0, LAN2 is 10.10.11.0.

The rules would be as follows:

Rule: R4
Direction: In
Private IP Type: Fixed
Protocol: TCP
Private IP Address: 10.10.10.4
Private IP Mask: 255.255.255.255
Private Port Range: HTTP
Public IP type: Dynamic
Public IP Address: <leave blank>
Public IP mask: <leave blank>
Public Port Range: 8080

Default Rules: Enabled Including IP Phones

Rule Order: R1,R2,R3,R4

NTP Client settings

Network Time Protocol (NTP) is an IP protocol that allows you to synchronize the time on your network devices. The NTP Client allows you to synchronize the time on your Business Communications Manager system with the NTP Server on your network. This ensures that your Business Communications Manager is using the same time as the other Business Communications Manager systems and servers on your network.

There are two clocks operating on the Business Communications Manager system.

Business Communications Manager system clock

The system clock is used for scheduled tasks and the time stamp on events and alarms. The NTP client synchronizes the system clock with the NTP server time.

Business Communications Manager telephony clock

The telephony clock provides the time that appears on the Business Communications Manager telephones. The telephony clock gets its time updates from the system clock. Due to delays in the system, there may be a difference between the system time and the time that appears on the telephones.

Configuring the NTP Client settings

1. On the navigation tree, click the **Services** key and click the **NTP Client Settings** heading. The NTP Client Settings screen appears.
2. Configure the NTP Client settings according to the following table.

Attribute	Description
NTP Server Address	Enter the IP address of the NTP Server to which you are synchronizing the Business Communications Manager time.
Maximum Time Adjustment	Enter the maximum time adjustment in seconds. If the time difference between Business Communications Manager and the NTP Server is greater than the maximum time adjustment, the time is **not** changed. Nortel Networks recommends that you use the default value of 0. A value of 0 allows the time to be changed regardless of the time difference.
Exit After Setting Time Once	Select whether the NTP Client exits after a time adjustment. Choose **Enabled** if you want the NTP Client Service to stop after a time adjustment is made. When you choose Enabled, the time is set only once. Choose **Disabled** if you want the NTP Client Service to continue running after a time adjustment is made.
Set Time Every	Enter the number of seconds between time updates. The default is 86400 seconds (24 hours). **Tip**: An event is entered into the Event Log each time Business Communications Manager accesses the NTP server to check for a time update. If you enter a short time period in this field, the Event Log will quickly fill with VoiceTimeSynch events.

Attribute	Description
Minimum Time Adjustment	Enter the time difference that must exist between the Business Communications Manager and the NTP Server before a time adjustment is made. If the time difference is less then the number of seconds entered, the time on the Business Communications Manager is not changed.
NTPClient Service Start Type	Select whether the NTP Client Service starts automatically. Choose **Automatic** if you want the NTP Client Service to start automatically when Business Communications Manager is started up or rebooted. Choose **Manual** if you want to start the NTP Client Service manually. For information on how to start the NTP Client Service, refer to "Starting the NTP Client Service" on page 423.

3 Press the **Tab** key to save your settings.

After you have configured the NTP Client settings, you must start the NTP Client service before the time adjustments will begin.

Starting the NTP Client Service

You must start the NTP Client Service the first time you configure the NTP Client settings. Also, if you have set the NTP Client Service Start Type option to Manual, you must start the NTP Client Service every time you want to update the Business Communications Manager time.

To start the NTP Client Service:

1 On the navigation tree, click the **Diagnostics** key and the **Service Manager** heading. The Service List screen appears.

2 Scroll down the list of until the VoiceTimeSynch service appears.

3 Click the **VoiceTimeSynch** service.

4 On the **Configuration** menu, click **Modify Services**. The Services List dialog box appears.

5 Configure the settings according to the following table.

Attribute	Description
Startup	Select whether the NTP Client Service starts automatically. Choose **Automatic** if you want the NTP Client Service to start automatically when Business Communications Manager is started up or rebooted. Choose **Manual** if you want to start the NTP Client Service manually. Choose **Disabled** to disable the NTP Client Service.
Status	Allows you to view and change the status of the NTP Client Service. Choose **Start** to start the NTP Client Service. When the service successfully starts, the status changes to Running. Choose **Stop** to stop the NTP Client Service. When the service successfully stops, the status changes to Stopped.

6 Click the **Save** button.

Chapter 18
Virtual Private Networks (VPN)

Business Communications Manager uses the Internet and tunneling protocols to create secure extranets. These secure extranets require a protocol for safe transport from the Business Communications Manager to another device through the Public Data Network (PDN). Business Communications Manager uses the PPTP and IPSec tunneling protocols. Both of these protocols have encryption, but IPSec has a slightly more secure hashing algorithm for negotiating keys.

Extranets can connect:

- mobile users to a fixed private network at their office over the PDN
- private networks in the two branch offices of the same corporation over PDN
- two divisions of the same corporation over the corporate intranet

When connecting two branch offices, the use of a VPN over the public data network is very efficient if the connection is required only intermittently or a dedicated point-to-point link is considered too expensive. Also, with the advent of business-to-business solutions, VPNs can be deployed to provide secure connections between corporations.

PPTP tunnels are used when a mobile user wishes to connect securely to a Business Communications Manager or when using the IPX network protocol. PPTP client software is required to use a PPTP tunnel. This client software is available for all personal computer operating systems from Microsoft. This client is included in Windows 98.

PPTP tunnels are created from a client to a server or from a server to a server. To form an extranet using PPTP, a mobile, remote user does the following:

- Establishes a connection with the public data network's point-of-presence (POP), typically through an Internet service provider (ISP) using dial up links.
- After the Internet connection is up, the remote user launches a second connection which is a VPN tunnel to Business Communications Manager. The Business Communications Manager public IP address is used to establish the tunnel.
- On the Business Communications Manager, the user id of the incoming user is enabled for dial-in access.

In the IPSec Specification, there are two tunnel modes defined: tunnel mode and transport mode. Business Communications Manager supports only tunnel mode. Tunnel mode describes a method of packetizing TCP/IP traffic to create a virtual tunnel.

Tunnels are created between servers, which are also known as gateways. This is called a Branch Office Connection. The end nodes connect to each other through gateways. These gateways set up the tunnel over the PDN on behalf of the end nodes. The establishment of the tunnel, and the PDN in between, is transparent to the end nodes which behave as if they are interacting through a router. Typically, the edge devices connecting the branches of a corporation to the ISP use VPN in this mode.

Business Communications Manager is compatible with the Contivity Extranet Switch and the Shasta 5000.

The following sections describe configuring the tunnel portion of Business Communications Manager using PPTP or IPSec.

PPTP

PPTP is a tunneling protocol supported by Nortel Networks, Microsoft, and other vendors. The PPTP client is available for Windows 95 (www.microsoft.com) and is built-in to Windows 98 and later. Third-party vendors have developed PPTP clients for Windows 3.1 and the Macintosh operating system.

The PPTP client and PPTP server software are components on Business Communications Manager.

PPTP offers the following features:

- Support for multiple authentication schemes: MS-CHAP, CHAP, or PAP.
- Support for IP address translation via encapsulation.
- Support for IPX tunneling.
- Support for RC4 encryption.
- Support for compression of data packets.

Settings required for PPTP tunnels

The data packets that pass through PPTP tunnels interact with other routing features in Business Communications Manager. As a result, there are several settings you must make in other features for PPTP tunnels to operate.

NAT (Network Address Translation)

On all of the interfaces expected to carry PPTP tunnel traffic, add rules to allow PPTP traffic (bidirectional traffic on TCP port 1723 and IP sub-protocol 47) to and from Business Communications Manager.

You cannot set NAT rules on traffic that goes through the PPTP tunnel. You can set NAT rules for the end points of the PPTP tunnel.

For information about how to change the NAT settings, refer to “NAT (Network Address Translation)” on page 416.

QoS

You cannot set QoS rules on traffic that goes through the PPTP tunnel. You can set QoS rules for the end points of the PPTP tunnel.

IP Routing and IPX Routing

Do not create a static route to the far end of the tunnel. If you do, packets will not be sent through the tunnel. PPTP sets up the necessary routes when the tunnel is enabled.

Filters

You must set the following parameters in IP Firewall filter programming.

- Allow GRE protocol (protocol ID 47) under IP for traffic to and from Business Communications Manager.
- Allow traffic to and from Business Communications Manager on the PPTP port (1723/tcp).

You cannot set IP Firewall filter rules on traffic that goes through the PPTP tunnel.You can set IP Firewall filter rules for the end points of the PPTP tunnel.

For information about how to change Filters, refer to "IP Firewall Filters" on page 470.

IP Addresses and DHCP Server

Ensure that the IP addresses for the LAN interfaces, WAN interfaces, dial up links, and PPTP tunnels are unique across all sites. This simplifies configuration, eliminates conflicts due to NAT, and prevents the addresses assigned by the DHCP server from conflicting with the IP addresses of subnets in remote sites.

For information on how to change the DHCP Server settings, refer to the DHCP section.

DNS Server

We recommend the following configuration if you are using a DNS Server:

- Choose one of the offices to act as the primary office. The server in primary office must have a dedicated link to the Internet.
- Make the server in the primary office the primary domain server. Ensure the DNS Server in the primary office contains all of the entries for allow the branch offices.
- Configure the DNS Servers in the branch offices to run in cache mode only. Allow a larger time out value on the branch DNS servers to accommodate for on-demand setup of PPTP tunnels to the primary office.
- Configure the branch DNS servers to forward DNS Server requests to the Internet Service Provider first and then to the DNS Server in the primary office.

For information on how to configure the DNS proxy service on Business Communications Manager, refer to the "DNS" on page 372.

Changing the PPTP settings

The settings of the PPTP Summary screen apply to all of the PPTP tunnels created.

To change the PPTP settings:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** heading.
   The PPTP Summary screen appears.
3. Configure the PPTP Summary settings. These settings are described in the following table.

Attribute	Description
Description	Displays the name of the PPTP service. This is a read only attribute.
Version	Displays the version number of the PPTP service. This is a read only attribute.
Keep Alive Interval	Allows you to specify the amount of time Business Communications Manager waits without any data traffic on the tunnel before it sends an Echo Request message. When the far end of the tunnel receives an Echo Request, the system at the far end must send an Echo Response message. If the far end of the tunnel sends an Echo Response message, Business Communications Manager keeps the tunnel open. If the far end of the tunnel does not send an Echo Response message, the tunnel is closed. You can enter a value from 1 to 65000 seconds. The default value is 60 seconds.
Echo Timeout	Allows you to specify the amount of time Business Communications Manager waits for an Echo Response message. If the Echo Response message is not received before this time limit, Business Communications Manager tears down the PPTP tunnel. You can enter a value from 1 to 65000 seconds. The default value is 60 seconds.
Max TCP Retransmissions	Allows you to specify the maximum number of times TCP retransmits the data packets. Data packets are retransmitted when the far end of a TCP connection does not acknowledge the receipt of a data packet. Business Communications Manager uses a TCP connection to establish a PPTP tunnel. The tunnel establishment packets may get lost while being transported over busy internet, effecting the private network connectivity between sites. Therefore, it is recommended to tune this parameter according to the performance of the internet carrying the PPTP tunnel traffic. You can enter a value from 1 to 65000 packets. The default value is 9 packets. **Note**: If you change this value, you must reboot Business Communications Manager.
Client IP Authentication	Allows to enable or disable Client Authentication. When Client Authentication is enabled, only clients entered on the Client List screen can open a PPTP tunnel. When Client Authentication is disabled, any client with valid credentials can open a PPTP tunnel. Note that valid credentials are required for clients on the Client List as well. You can choose Enabled or Disabled. The default value is Disabled. **Note**: If you change this value, you must reboot Business Communications Manager.

4. Click the **Tab** key to save the settings.

Adding a PPTP Client

A PPTP Client is a remote Business Communications Manager or other similar PPTP capable device that you allow to connect to this Business Communications Manager to establish a PPTP tunnel.

The maximum number of PPTP clients is 32.

To add a PPTP client:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** heading.
   The PPTP Summary screen appears.
3. Click the **Clients IP List** tab.
   The Clients IP List screen appears.
4. On the **Configuration** menu, click **Add to Client IP List**.
   The Client IP dialog box appears.
5. Configure the PPTP Client attributes. These attributes are described in the following table.

Attribute	Description
Client	Allows you to specify the Client identifier. The Client setting uniquely identifies a PPTP client. The value for this setting must follow certain conventions. You must type the prefix 'C' followed by a unique number identifying the PPTP client. For example, 'C2' is a valid name. If you specify an existing client name, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The client identifier does not have any significance, other than uniquely identifying an entry. The m
Client IP Address	Enter the IP address of the system you are allowing to use a PPTP tunnel to connect to Business Communications Manager. Enter the IP address in the dotted format.

6. Click the **Save** button.

Deleting a PPTP client

To delete a PPTP client:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** heading. The PPTP Summary screen appears.
3. Click the **Clients IP List** tab. The Clients IP List screen appears.
4. Click the PPTP client you want to delete.
5. On the **Configuration** menu, click **Delete From Client IP List**.
   A message prompts you to confirm the deletion.
6. Click the **Yes** button to confirm the deletion.

Adding a PPTP tunnel

You can create a PPTP tunnel from a Business Communications Manager system to another Business Communications Manager system or from a Business Communications Manager system to a Contivity Extranet Switch.

Note: When you create a PPTP tunnel, a user profile is created for the tunnel. This user profile is the profile a person uses when they connect to Business Communications Manager using this tunnel. The user name for the profile created is the same as the interface name for the PPTP tunnel.

The maximum number of PPTP tunnels running at one time is 10.

To add a PPTP tunnel:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** heading.
   The PPTP Summary screen appears.
3. Click the **Add** menu.
   Or, right click the PPTP heading and click **Add**.
   The Add PPTP dialog box appears.
4. Configure the PPTP tunnel attributes. These attributes are described in the following table.

Attribute	Description
Tunnel Name	Allows you to specify the name that is used to identify this tunnel. This name is the User ID for the remote end of the tunnel. For information about the User ID, refer to "User ID" on page 433.
Incoming Password	Allows you to specify the password used by the other end of the tunnel to connect to this PPTP tunnel on this Business Communications Manager.
Confirm Incoming Password	Allows you to re-enter the incoming password to confirm that you have entered the password correctly.
Port Name	Allows you to specify the VPN port that this PPTP tunnel will use. Several PPTP tunnels can be assigned a single VPN port, however only one PPTP tunnel can use the port at a time. To avoid port contention, choose a VPN port that is not frequently used by other PPTP tunnels.

5. Click the **Save** button to add the tunnel.

Configuring a PPTP tunnel

After you have added the PPTP tunnel you need to configure the PPTP settings. To configure a PPTP tunnel:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** key.
3. Click the PPTP tunnel you want to configure.
   The Tunnel Summary screen appears.
4. Configure the Tunnel Summary attributes. These attributes are described in the following table.

Attribute	Description
Interface	Displays the name used to identify this tunnel.
IP Address Mode	Allows you to specify if the IP address for this PPTP tunnel is assigned locally using the Unified Manager (Local-Fixed) or is assigned by the remote device automatically (RemoteAssigned). If you choose RemoteAssigned, this end of the tunnel requests for an IP address during tunnel establishment. The PPTP server component on the remote end of the tunnel provides one either from its local pool or from a DHCP server running in that site.
IP Address	Allows you to specify the IP address assigned to this PPTP tunnel. Enter the IP address in the dotted format. Do not enter an IP address if the IP Address Mode is set to RemoteAssigned.
Description	Allows you to enter a brief description of the PPTP tunnel.
Status	Displays the current status of the PPTP tunnel. The status can be Disabled, Up, Down. You can change the status of the PPTP tunnel by selecting **Disabled** or **Enabled**. When the tunnel is Enabled, it is normally in the Up state or in the Down state. You can change it to Up state to connect the tunnel manually and to Down state to disconnect the tunnel manually - irrespective of the Tunnel Link attributes. **Note**: You cannot Disable the tunnel when the status is UP. To Disable the tunnel, you must: 1. Stop all traffic through the tunnel. 2. Change the status to Down. 3. Change the status to Disabled.

5. Click the **Tunnel Link Parameters** tab.
   The Tunnel Link Parameters screen appears.
6. Configure the Tunnel Link Parameters. These parameters are described in the following table.

Attribute	Description
Remote PPTP Server - Primary	Allows you to specify the IP address of the primary PPTP server to which this tunnel connects. Enter the IP address in the dotted format. A DNS name of the PPTP server can be specified for this attribute. However, it takes longer to establish a PPTP tunnel since a DNS resolution must happen first. In branch configurations, the actual DNS server may reside in another location which could cause the DNS resolution to take even more time. Therefore, it is recommended that IP addresses in dotted decimal format be specified for Primary PPTP Server and the Secondary PPTP Server, if it exists.
Remote PPTP Server - Secondary	Allows you to specify the IP address of the PPTP server to which this tunnel connects when the primary server is not available. Enter the IP address in the dotted format.

Attribute	Description
Connect retries	Allows you to specify the maximum number of times this tunnel attempts to connect to the primary PPTP server. If a connection is not made after the specified number of retries, this tunnel attempts to connect to the secondary PPTP server. If a connection to the secondary PPTP server is not made after the specified number of retries, the tunnel connection fails. Enter a value from 0 to 10. If you enter a value of 0, Business Communications Manager does not try to connect again.
Retry interval	Allows you to specify the number of seconds Business Communications Manager waits between connect retries. Enter a value from 1 to 3600000 seconds.
Connection type	Allows you to specify when the tunnel is established and when it is torn down. A **Persistent** tunnel is brought up as soon as the Business Communications Manager starts. The tunnel remains connected until Business Communications Manager shuts down or an administrator manually disconnects the tunnel by changing the status to Down. An **On Demand** connection is established only when the connectivity provided by it is needed. Administrators specify the destination networks reachable through a tunnel in the Destination Networks tab. When a packet bound for any of those destinations reaches this Business Communications Manager, Business Communications Manager brings up this tunnel. An On Demand tunnel is torn down when an administrator manually changes its status to Down or after the Idle Timeout period as expires.
Idle timeout	Allows you to specify how long Business Communications Manager waits when there is no traffic on the tunnel before the PPTP tunnel is torn down. Idle timeout only applies to tunnels that have a Connection type of on-demand. Persistent PPTP tunnels are not automatically torn down. Enter a value from 0 to 32000 seconds. A value of 0 disables automatic tear down of the tunnel
Data Compression	Allows you to specify if the data sent in this tunnel is compressed. Select Enabled or Disabled.

7 Click the **Tunnel Authentication Parameters** tab.
The Tunnel Authentication Parameters screen appears.

8 Configure the Tunnel Authentication Parameters. These parameters are described in the following table.

Attribute	Description
Authentication type	Allows you to specify the type of authentication is used for this tunnel. You can select: AllowClearText (PAP authentication), EncryptedOnly (CHAP authentication) or Microsoft Encrypted Only (MS-CHAP). It is recommended that you use MS-CHAP if you are using Data Encryption.
Two Way Authentication	Allows you to enable or disable two way authentication for this tunnel. If you disable two way authentication, the client sends authentication parameters to the server and server verifies the parameters. If you enable two way authentication, the server verifies the client and the client verifies the server.
Data encryption	Allows you to specify the encryption method used for tunneled data. You can choose no encryption (Disabled) or 40-bit encryption (Enabled).

Attribute	Description
User ID	Allows you to specify the User ID that this end of the tunnel sends to the far end of the tunnel for authentication during tunnel establishment. If you are using another Business Communications Manager on the far side of the tunnel, this User ID needs to match the tunnel name or interface name specified on the far side of the tunnel. If you are not using another Business Communications Manager on the far side, then this User ID must satisfy the authentication and other criteria for that device.
Password	Allows you to specify the password used to authenticate with the far side of the tunnel. If PAP is being used, this value is treated as simple password. If CHAP or MS-CHAP is used, this value is used as the CHAP secret and the actual password is not passed over the link. Not sending the actual password provides extra security. This value must match the 'Incoming Password' value specified for the tunnel on the far end.

9 Click the **Destination Networks** tab.
The Destination Networks screen appears.

From the Destination Networks screen you can add, modify and delete Destination Networks.

To add a Destination Network

The maximum number of Destination Networks is 128.

1 On the **Configuration** menu, click **Add Destination Network**.
The Destination Networks screen appears.

2 Configure the Destination Networks attributes. These attributes are described in the following table.

Attribute	Description
Entry (N#)	Allows you to specify the Destination Network identifier. The Entry setting uniquely identifies a Destination Network. The value for this setting must follow certain conventions. You must type the prefix 'N' followed by a unique number identifying the Destination Network. For example, 'N2' is a valid name. If you specify an existing Destination Network, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Destination Network identifier does not have any significance, other than uniquely identifying an entry.
Destination Network	Allows you to enter the IP address of the network or hosts that can be reached through this PPTP tunnel. These IP addresses correspond to the private LAN addresses in the remote sites connected by this tunnel. When this Business Communications Manager receives a data packet from the networks behind it with destination address in these destination networks, Business Communications Manager routes those packets through this tunnel. If this tunnel is not active, it is automatically brought up. Note that Destination Networks are not necessary for persistent connections. Enter the IP Address of the destination network in the remote site in dotted notation.
Subnet Mask	Allows you to specify the subnet mask for the destination network. You require Subnet Mask only if you have entered a value in the Destination Network box. Always use a valid subnet address and mask pair. If you are using a mask that contains more than 1 host address, then always specify the subnet number that corresponds to that subnet and not any other address. For example, if you are using a mask of 24 bits, (255.255.255.0) then use a subnet number of 192.168.100.0 and not something like 192.168.100.11 (where the last number should have been 0). Enter the subnet mask in the dotted format.

Attribute	Description
Preference Level	Allows you to specify the preference level for this tunnel. When there are multiple tunnels assigned to a destination network, the preference level determines which tunnel is used to connect to the destination network. Business Communications Manager attempts to use the tunnel with the lowest preference number first. If the connection fails, Business Communications Manager retries the connection as many time as is specified in the Connect retries box on the Tunnel Link Parameters screen. After the specified number of retries fails, Business Communications Manager attempts to use the tunnel with the next lowest preference level. Business Communications Manager continues to attempt to establish a tunnel until a connection succeeds or all of the tunnels to the destination network have failed. For example, a site may have two connections to the internet to take advantage of varied capacities and costs. You can maintain a PPTP server at each of these connection points. When you are specifying PPTP tunnels to reach private networks in this site, you may want to use the connection that is most cost-effective first and use the other connection only if the most cost effective connection is not in service. To do this, you create two tunnels to reach the site. You specify the corresponding PPTP server addresses for each tunnel, but enter the same destination addresses (unless you want to distinguish between the normal and stand-by operation). However, for the most desired connection to the site, you specify higher precedence level for the tunnel by putting a lower value for Preferred Level than for the other tunnel. When a packet is received by Business Communications Manager with the destination address of this site, Business Communications Manager tries to bring up the most desired tunnel. If the connection succeeds, tunnel is established. If Business Communications Manager cannot connect to this tunnel after the specified number of retries, it attempts to bring up the 'less desired' tunnel using its parameters. This feature is useful for providing redundant links to sites that have multiple connections to the internet. Note that this parameter is only used with On Demand tunnels.

3 Click the **Save** button.

To modify a Destination Network

1 Click the Destination Network to modify.

2 On the **Configuration** menu, click **Modify Destination Network**.
The Destination Networks screen appears.

3 Change the Destination Networks attributes.

4 Click the **Save** button.

To delete a Destination Network

1 Click the Destination Network to delete.

2 On the **Configuration** menu, click **Delete Destination Network**.
A message prompts you to confirm the deletion.

3 Click the **Yes** button to confirm the deletion.

Deleting a PPTP tunnel

Note: Before you delete a PPTP tunnel, delete any destination networks assigned to the tunnel.

To delete a PPTP tunnel:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **PPTP** key.
3. Click the PPTP tunnel you want to delete.
   The Tunnel Summary Parameters screen appears.
4. Click the **Delete** menu.
   Or, right click the PPTP heading and click **Delete**.
   A message prompts you to confirm the deletion.
5. Click the **Yes** button to confirm the deletion.

Note: When you delete a PPTP tunnel, the user profile for the tunnel is not deleted. Since the user profile has dial-in permission, a person at the remote end can still access the Business Communications Manager system using this user profile. To prevent dial-in access from the remote site, you must also delete the user profile that has the same user name as the interface name for the PPTP tunnel. For information about how to delete a user profile, "User Manager" on page 479.

IPSec

The IPSec standard defines a set of security protocols that authenticate IP connections and add confidentiality and integrity to IP packets. IPSec packets are transparent to applications and the underlying network infrastructure. IPSec supports various encryption and authentication protocols so that your security policy can dictate levels of data privacy and authentication.

IPSec uses a flexible key management scheme called the Internet Security Association Key Management Protocol (ISAKMP), which enables peer connections to quickly and dynamically agree on compatible security and connection parameters (keys, encryption, and authentication).

Encryption

All of the following encryption methods ensure that the packets have come from the original source at the secure end of the tunnel. Note that some of the encryption types will not appear on some non-US models that are restricted by US Domestic export laws.

The following table shows a comparison of the security provided by the available encryption and authentication methods.

Table 164 Comparing Encryption and Authentication Methods

Method (strongest to weakest)	Encryption of IP Packet Payload	Authentication of IP Packet Payload	Authentication of Entire IP Packet
ESP Triple DES SHA1	Yes	Yes	No
ESP Triple DES MD5	Yes	Yes	No
ESP 56-bit DES SHA1	Yes	Yes	No
ESP 56-bit DES MD5	Yes	Yes	No
ESP 40-bit DES SHA1	Yes	Yes	No
ESP 40-bit DES MD5	Yes	Yes	No
AH HMAC SHA1	No	No	Yes
AH HMAC MD5	No	No	Yes

Note: Using higher-level encryption, such as Triple DES, requires more system resources and increases packet latency. You need to consider this when designing your overall network.

Note: If two devices have different encryption settings, the two devices will negotiate downward until they agree on a compatible encryption capability. For example, if Switch A attempts to negotiate Triple DES encryption with Switch B that is using 56-bit DES, then the Switch B will reject Triple DES encryption in favor of the 56-bit DES.

The encryption level you choose is made of three components:

- the protocol
- the encryption method
- the authentication method

Protocol

The protocol can be ESP or AH.

- ESP
  Encapsulating Security Payload (ESP) provides data integrity, source authentication and confidentiality for IP datagrams by encrypting the payload data to be protected. ESP uses the Data Encryption Standard (DES) and Triple DES algorithms.
- AH
  Authentication Header (AH) provides data integrity and source authentication. The AH method does not encrypt data. The use of a NAT device in the tunnel path can sometimes cause the AH method to report a security violation.

Encryption method

The encryption method can be Triple DES, 56-bit DES or 40-bit DES. Triple DES is the strongest encryption and 40-bit DES is the weakest encryption.

- Triple DES
  Triple DES is an encryption block cipher algorithm that uses a 168-bit key. It uses the DES encryption algorithm three times. The first 56 bits of the key is used to encrypt the data, then the second 56 bits is used to decrypt the data. Finally, the data is encrypted once again with the third 56 bits. These three steps triple the complexity of the algorithm.
- 56-bit DES
  56-bit DES is an encryption block cipher algorithm that uses a 56-bit key (with 8 bits of parity) over a 64-bit block. The 56 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps.
- 40-bit DES
  40-bit DES is an encryption block cipher algorithm that uses a 40-bit key (with 8 bits of parity) over a 64-bit block. The 40 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps. Both 40- and 56-bit DES require the same processing demands, so you should use 56-bit DES unless local encryption laws prohibit doing so.

Authentication method

The authentication method can be SHA1 or MD5.

- SHA1
  Secure Hash Algorithm (SHA1) produces a 160-bit hash. It is regarded by cryptographers as being more resistant to attacks than MD5. SHA1 does not encrypt data.
- MD5
  Message Digest 5 (MD5) Algorithm produces a 128-bit hash. It is used to confirm the authenticity of a packet. MD5 does not encrypt data. Also, MD5 provides integrity that detects packet modifications.

Both SHA1 and MD5 use Hashed Message Authentication Code (HMAC) to improve authentication. HMAC is a technique that uses a secret key and a message digest function to create a secret message authentication code.

Settings required for IPSec tunnels

The data packets that pass through IPSec tunnels interact with other routing features in Business Communications Manager. As a result, there are several settings you must make in other features for IPSec tunnels to operate.

NAT (Network Address Translation)

On all of the interfaces expected to carry IPSec tunnel traffic, add rules to allow IPSec traffic (bi-directional traffic on TCP port 500 and IP sub-protocols 50 and 51) to and from Business Communications Manager.

For information about how to change NAT parameters, refer to "NAT (Network Address Translation)" on page 416.

Filters

You must set the following parameters in IP Firewall Filters programming.

- Allow IPSec protocols (protocol ID 50 for AH and 51 for ESP) under IP for traffic to and from Business Communications Manager.
- Allow traffic to and from Business Communications Manager on the IPSec port (500/tcp).

For information about how to change Filters, refer to "IP Firewall Filters" on page 470.

Routing

Routes must be set to reach the Remote Accessible Networks. IPSec does not set these routes automatically.

Dialup ISDN connections

When you are creating an IPSec tunnel over a Dialup ISDN connection, the endpoint must have a fixed IP address.

Compatibility with Contivity Extranet Switch and Shasta 5000

When connecting to a Contivity Extranet Switch, you must disable Vendor ID and Compression under Base Class on the Contivity Extranet Switch.

Business Communications Manager does not support the IPSec RIP implementation used by the Contivity Extranet Switch. Use Static Routes when connecting to the Contivity Extranet Switch.

When connecting to a Shasta 5000, you must set the PFS to No on the Tunnel configuration of Business Communications Manager.

IPSec and PPTP

The Remote Accessible Networks of an IPSec tunnel cannot be the same as a Destination Network on a PPTP tunnel. The Remote Endpoint of an IPSec tunnel's Remote Endpoint cannot be the same as a Destination Endpoint on a PPTP tunnel.

Changing the IPSec global settings

The IPSec global settings apply to all of the IPSec tunnels.

To change the IPSec global settings:

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** heading.
   The Global Settings screen appears.
3. Configure the IPSec global settings. These settings are described in the following table.

Attribute	Description
Description	Displays the name of the IPSec service. This is a read only attribute.
Version	Displays the version number of the IPSec service. This is a read only attribute.
Encryption	Allows you to select the encryption levels that you allow your IPSec tunnels to use. The encryption level used for the IPSec tunnel is negotiated when the tunnel is opened. The encryption levels you select are the encryption levels that you allow Business Communications Manager to use for IPSec tunnels. This is a global setting that applies to all of the IPSec tunnels on Business Communications Manager. When you add an IPSec tunnel, you can further restrict the encryption levels for each tunnel. For more information, refer to "Adding an IPSec Tunnel" on page 440. For a description of the encryption levels, refer to "Encryption" on page 436.
Status	Allows you to enable or disable the use of IPSec tunnels. You can choose Enabled or Disabled. The default value is Disabled.

4. Click the **Tab** key to save the settings.

Adding an IPSec Tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** heading.
   The Global Settings screen appears.
3. Click the **Add** button.
   Or, right click the **IPSec** heading and click **Add**.
   The Add IPSec dialog box appears.
4. Configure the Tunnel Settings. These settings are described in the following table.

Attribute	Description
Tunnel Number	Allows you to specify the Tunnel identifier. The Tunnel Number uniquely identifies a IPSec tunnel. The value for this setting must follow certain conventions. You must type the prefix 'T' followed by a unique number identifying the IPSec Tunnel. For example, 'T2' is a valid name. If you specify an existing Tunnel number, you receive an error message. The client identifier does not have any significance, other than uniquely identifying an entry. The maximum number of tunnels you can add is 20.
IPSec Enabled	Allows you to enable this IPSec tunnel. You can choose Yes or No. The default setting is Yes.
PFS Enabled	Allows you to enable Perfect Forward Secrecy (PFS). With PFS, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys. If you create a tunnel to a Contivity Extranet Switch, you must set PFS Enabled to Yes. You can choose Yes or No. The default setting is Yes. **Note**: Set PFS to No for connections to the Shasta 5000.
Idle Timeout	Allows you to specify the amount of time the tunnel can remain idle before the tunnel is closed. You cannot set the Idle Timeout setting to less than three minutes, except to disable the timeout by entering 00:00:00. Enter a value from 00:03:00 to 23:59:59. The default setting is 00:15:00. A setting of 00:00:00 disables the Idle Timeout setting.
Highest Encryption	Allows you to select the highest encryption level allowed on this IPSec tunnel. When the encryption level is negotiated for this tunnel, Business Communications Manager will not use any encryption level higher than the encryption level specified in this field. For a description of the encryption levels, refer to “Encryption” on page 436.
Key Type	Select the format for the Preshared Key. The Key Type must be the same on both ends of the IPSec tunnel. The format can be text or hexadecimal. Note: If you change the Key Type, the Preshared Key is deleted.
Preshared Key	Allows you to specify the text or hexadecimal string used to authenticate the data sent on this tunnel. The maximum length of the Preshared Key is 32 characters. This key must be used at both ends of the IPSecTunnel. For best security, use a secure method to share this key.
Confirm Preshared Key	Allows you to re-enter the Preshared Key to confirm that you entered the key correctly.

Attribute	Description
Rekey Timeout	Allows you to specify the amount of time you can use a key before the tunnel is re-negotiated. You should limit the lifetime of a single key used to encrypt data or else you will compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys are exchanged between servers. You cannot set the Rekey Timeout setting to less than three minutes, except to disable the timeout by entering 00:00:00. Enter a value from 00:03:00 to 23:59:59. The default setting is 08:00:00. A setting of 00:00:00 disables the Rekey Timeout setting.
Rekey Data Count	Allows you to specify the amount of data you can transmit on the tunnel before the tunnel is re-negotiated. Enter a value from 0 to 1000000 Kbytes. A setting of 0 disables the Rekey Data Count. **Note**: If you set the Rekey Data Count too low, the tunnel is re-negotiated too often and will consume extra system resources.
Local Endpoint	Allows you to specify the IP address of the interface on Business Communications Manager that is the entrance or exit of the IPSec tunnel. Enter the IP address in the dotted format.
Remote Endpoint	Allows you to specify the IP address of the remote IPSec gateway that is the entrance or exit of the IPSec tunnel. Enter the IP address in the dotted format. **Note**: Different tunnels cannot have the same Remote Endpoint. This includes PPTP tunnels.

5 Click the **Save** button.

Adding Local Accessible Networks to the IPSec tunnel

The maximum number of Local Accessible Networks you can add is 16.

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the tunnel you want to modify.
The Tunnel Parameters screen appears.

3 Click the **Local Accessible Networks** tab.
The Local Accessible Networks screen appears.

4 On the **Configuration** menu, click **Add Local Accessible Network**.

5 Configure the Local Accessible Network parameters. These parameters are described in the following table.

Attribute	Description
Network Number (L#)	Allows you to specify the Network identifier. The Network Number uniquely identifies a Local Accessible Network. The value for this setting must follow certain conventions. You must type the prefix 'L' followed by a unique number identifying the Local Accessible Network. For example, 'L2' is a valid name. If you specify an existing Network number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Network identifier does not have any significance, other than uniquely identifying an entry. The maximum number Local Accessible Networks you can add is 16.

Attribute	Description
IP Address	Allows you to specify the IP addresses of interfaces on Business Communications Manager that can connect to this tunnel. Enter the IP address in the dotted format.
IP Address Mask	Allows you to specify the subnet mask of interfaces on Business Communications Manager that can connect to this tunnel. Enter the Subnet Mask in the dotted format.

6 Click the **Save** button.

Adding Remote Accessible Networks to the IPSec tunnel

The maximum number of Remote Accessible Networks you can add is 16.

1 On the navigation tree, click the **Services** key and click the **VPN** key.

2 Click the **IPSec** key and click the tunnel you want to modify.
The Tunnel Parameters screen appears.

3 Click the **Remote Accessible Networks** tab.
The Remote Accessible Networks screen appears.

4 On the **Configuration** menu, click **Add Remote Accessible Network**.

5 Configure the Remote Accessible Network parameters. These parameters are described in the following table.

Attribute	Description
Network Number (R#)	Allows you to specify the Network identifier. The Network Number uniquely identifies a Remote Accessible Network. The value for this setting must follow certain conventions. You must type the prefix 'R' followed by a unique number identifying the Remote Accessible Network. For example, 'R2' is a valid name. If you specify an existing Network number, you receive an error message. If you use non-sequential numbers the system automatically reassigns sequential numbers. The Network identifier does not have any significance, other than uniquely identifying an entry. The maximum number of Remote Accessible Networks you can add is 16.
IP Address	Allows you to specify the IP addresses of IPSec gateways that you can connect to using this tunnel. Enter the IP address in the dotted format.
IP Address Mask	Allows you to specify the subnet mask of IPSec gateways that you can connect to using this tunnel. Enter the Subnet Mask in the dotted format.

6 Click the **Save** button.

Note: Different tunnels cannot have the same Remote Accessible Networks.

Modifying an IPSec Tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
3. Change the required IPSec Tunnel settings.
   For information about the settings refer to the table in the section "Adding an IPSec Tunnel" on page 440.
4. Click the **Tab** key to save your changes.

Modifying Local Accessible Networks to the IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
3. Click the **Local Accessible Networks** tab.
   The Local Accessible Networks screen appears.
4. Click the Local Accessible Network you want to modify.
5. On the **Configuration** menu, click **Modify Local Accessible Network**.
6. Modify the Local Accessible Network parameters.
7. Click the **Save** button.

Modifying Remote Accessible Networks to the IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
3. Click the **Remote Accessible Networks** tab.
   The Remote Accessible Networks screen appears.
4. Click the Remote Accessible Network you want to modify.
5. On the **Configuration** menu, click **Modify Remote Accessible Network**.
6. Modify the Remote Accessible Network parameters.
7. Click the **Save** button.

Deleting an IPSec Tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the tunnel you want to delete.
3. Click the **Delete** button.
   Or, right click the tunnel you want to delete and click **Delete**.
   A message prompts you to confirm the deletion.
4. Click the **Yes** button.

Deleting Local Accessible Networks to the IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
3. Click the **Local Accessible Networks** tab.
   The Local Accessible Networks screen appears.
4. Click the Local Accessible Network you want to delete.
5. On the **Configuration** menu, click **Delete Local Accessible Network**.
   A message prompts you to confirm the deletion.
6. Click the **Yes** button.

Deleting Remote Accessible Networks to the IPSec tunnel

1. On the navigation tree, click the **Services** key and click the **VPN** key.
2. Click the **IPSec** key and click the tunnel you want to modify.
   The Tunnel Parameters screen appears.
3. Click the **Remote Accessible Networks** tab.
   The Remote Accessible Networks screen appears.
4. Click the Remote Accessible Network you want to delete.
5. On the **Configuration** menu, click **Delete Remote Accessible Network**.
   A message prompts you to confirm the deletion.
6. Click the **Yes** button.

Creating a tunnel between two Business Communications Manager systems

The following is an example of a how to connect two Business Communications Manager systems together using an IPSec tunnel.

In this example, the IPSec tunnel connects a Business Communications Manager with a LAN 2 IP address of 10.10.11.1 and another Business Communications Manager with a LAN 2 IP address of 10.10.11.2. LAN 1 on the first Business Communications Manager is on the subnet 12.12.12.0. The LAN 1 of the second Business Communications Manager is on subnet 14.14.14.0.

On the first Business Communications Manager:

1. Set the Local Endpoint to **10.10.11.1**.
2. Set the Remote Endpoint to **10.10.11.2**.
3. Set the Preshared Key to **123**.
4. Set the Key Type to **Text**.
5. Set the Local Accessible Networks to **12.12.12.0** with mask **255.255.255.0**.
6. Set the Remote Accessible Networks to **14.14.14.0** with mask **255.255.255.0**.
7. Add a static route to 14.14.14.0, if this interface is not the default gateway.

On the second Business Communications Manager:

1. Set the Local Endpoint to **10.10.11.2**.
2. Set the Remote Endpoint to **10.10.11.1**.
3. Set the Preshared Key to **123**.
4. Set the Key Type to **Text**.
5. Set the Local Accessible Networks to **14.14.14.0** with mask **255.255.255.0**.
6. Set the Remote Accessible Networks to **12.12.12.0** with mask **255.255.255.0**.
7. Add a static route to 12.12.12.0, if this interface is not the default gateway.

On the Global settings for both Business Communications Manager systems, set the Status to Enabled.

Creating a tunnel between a Business Communications Manager and a Contivity Extranet Switch v02_61

The following is an example of a how to connect a Business Communications Manager to a Contivity Extranet Switch using an IPSec tunnel.

In this example, the IPSec tunnel connects a Business Communications Manager with a LAN 2 IP address of 47.81.20.50 and a Contivity Extranet Switch with a Public IP address of 47.82.30.60. LAN 1 on the Business Communications Manager is on the subnet 10.10.11.0. The Contivity Extranet Private LAN is on the subnet 14.14.14.0.

On the Business Communications Manager:

1. Set the Local Endpoint to **47.81.20.50**.
2. Set the Remote Endpoint to **47.82.30.60**.
3. Set the Preshared Key to **123**.
4. Set the Key Type to **Text**.
5. Set the Local Accessible Networks to **10.10.11.0** with mask **255.255.255.0**.
6. Set the Remote Accessible Networks to **14.14.14.0** with mask **255.255.255.0**.
7. Add a static route on LAN2 for the subnet 14.14.14.0 with the next hop as 47.82.30.50, if this interface is not the default gateway. For information about adding static routes, refer to “IP Routing” on page 374.

On the Contivity Extranet Switch:

1. Go to Profiles->Network and create a Network with the IP address 14.14.14.0 with mask 255.255.255.0. You will use this for the Local Accessible Networks for your Branch Office Connection.
2. Under Profiles->Branch Office, create a Group based on the Base class.
3. Under this new Group, change theVendor ID to Disabled and change Compression to Disabled. Business Communications Manager does not support Vendor ID or Compression.
4. Select Define Branch Office Connection.
5. Set the routing type to be Static.
6. Set the Local Endpoint to 47.82.30.60 and the Remote Endpoint to 47.82.20.50.
7. Under Local Accessible Networks, select the Network that was created earlier.
8. Set the Remote Accessible Networks to 10.10.11.0 with mask 255.255.255.0.
9. For the Preshared Key, select the Text button and set the key to '123'. This must match the BCM key.
10. Mark the box for Enable Branch Office Connection.

Chapter 19
Policy-enabled networking

This chapter discusses the services you can configure to enhance your data network.

Overview

Business Communications Manager enables system administrators to implement classes of service and assign priority levels to different types of traffic. Using Unified Manager, you can configure policies that monitor the characteristics of traffic (for example, its source, destination, and protocol) and perform a controlling action on the traffic when certain user-defined characteristics are matched.

Differentiated Services (DiffServ) overview

Differentiated services (DiffServ) is a Quality of Service (QoS) network architecture that offers varied levels of service for different types of data traffic. DiffServ lets you designate a specific level of performance on a packet-by-packet basis instead of using the “best-effort” model for your data delivery. You can give preferential treatment (prioritization) to applications that require high performance and reliable service, such as voice and video over IP.

Business Communications Manager includes the capability to enhance your network traffic management. For each packet, there is an octet in the packet header, the DiffServ (DS) field, that you can designate for specific service. For IP packets, six bits of the DiffServ field is the DiffServ Code Point (*DSCP)*. The DSCP value defines how the packet is to be treated as it travels through the network. You can set traffic criteria to match the DS field, and policy actions to change the DiffServ field to conform to various other mappings.

Business Communications Manager uses DiffServ to manage network traffic and resources. The information that is required to support DiffServ and multi-field classification is transferred using the Common Open Policy Services (COPS) protocol. COPS is a query and response protocol that exchanges policy information messages using the Transmission Control Protocol (TCP). All configuration can be performed using SNMP and Unified Manager.

DiffServ IP Quality of Service (QoS) architecture

DiffServ uses a simple mechanism that relies on a special encoding of the first 6 bits of the DiffServ byte in the IP header. This byte is the IPv4 Type of Service (ToS) byte; for IPv6, is the Traffic Class byte. The first 6 bits of this byte are called the DiffServ Code Point (DSCP).

In the packet forwarding path, differentiated services are processed by mapping the packet DSCP to a particular forwarding treatment, or per hop behavior (PHB), at each network node along its path. The code points may be chosen from a set of 32 standard values, a set of 16 recommended values to be used in the future, or a set of 16 values reserved for experimentation and local use. Of the 32 standard values, there are 8 Class Selector code points that are used primarily (but not exclusively) for backward compatibility with existing definitions of the ToS byte.

Business Communications Manager is a DiffServ node that can support DiffServ functions and behavior. DiffServ architecture defines a DiffServ-capable domain as a contiguous set of DiffServ-compliant nodes that operate with a common set of service provisioning policies and PHB definitions. The DiffServ domain is an autonomous system or network such as an internet service provider (ISP) network or campus LAN.

DiffServ assumes the existence of a service level agreement (SLA) between DiffServ domains that share a border. The SLA defines the profile for the aggregate traffic flowing from one network to the other based on policy criteria. In a given traffic direction, the traffic is expected to be shaped at the egress point of the upstream network and policed at the ingress point of the downstream network.

End-to-end QoS is enabled, typically through bilateral agreements (an agreement between two DiffServ domains), between all the domains from the sender to the receiver. These agreements aid in consistent PHB and QoS performance across all domains.

Typically, there are three types of edge devices in a DiffServ domain:

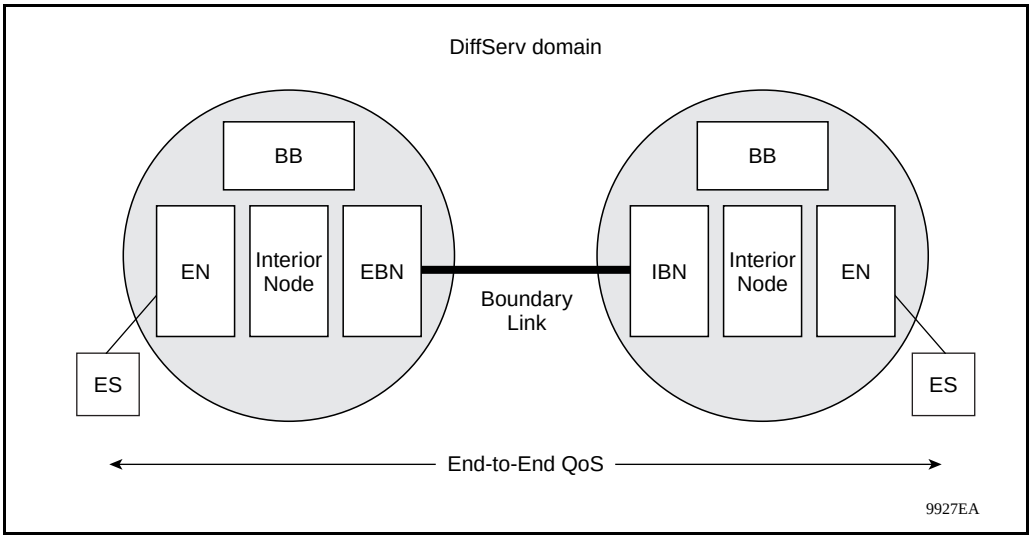
- Edge node (EN) — the switch or router connected directly to the desktop end station (ES) (Business Communications Manager is an edge node in the DiffServ domain)

  Ingress border node (IBN) — the ingress router at the boundary between two DiffServ domains

- Egress border node (EBN) — the egress router at the boundary between two DiffServ domains

Figure 54 shows the bandwidth broker and various DiffServ nodes in two DiffServ domains.

Figure 54 DiffServ bandwidth brokers and nodes



DiffServ components

The DiffServ architecture is comprised of the following components:

- Traffic conditioners — These components include classifiers, DiffServ-byte markers, shapers, policiers and profilers. Marking is performed at network boundaries, including the edges of the network (first hop router or switch or source host) and administrative boundaries between networks or autonomous systems. Traffic conditions should exist at DiffServ ingress and egress nodes. Business Communications Manager is an edge switch that supports packet classification based on header information in layer 3 and layer 4 of the Open System Interconnection (OSI) layering model. Business Communications Manager can mark and re-mark IP traffic based on the policies you define.
- Packet schedulers and queue managers — PHBs are expected to be implemented by employing a range of queue service and/or queue management disciplines on a network node output interface queue (for example, weighted fair queueing or drop preference queue management). DiffServ does not require a particular discipline for queue management or servicing to realize a particular service. All DiffServ nodes should support the packet scheduling and queue management algorithms that are necessary to implement the required PHB.

  Business Communications Manager supports a queue service discipline that allows packets to be serviced in an absolute priority fashion or using a weighted fair queueing scheduler. This service discipline ensures that packets in the highest-priority queue are serviced quickly without starving lower-priority queues.
- Bandwidth brokers (not supported in Business Communications Manager) — Bandwidth brokering is responsible for bandwidth allocation, QoS policy management, and flow admission control in a given DiffServ domain. Business Communications Manager does not support bandwidth brokering or traffic admission control.

IP service classes

Business Communications Manager supports the following services classes:

- Critical and Network classes have the highest priority over all other traffic.
- Premium class is an end-to-end service functioning similarly to a virtual leased line. Traffic in this service class is guaranteed an agreed upon peak bandwidth. Traffic requiring this service should be shaped at the network boundary in order to undergo a negligible delay and delay variance. This service class is suitable for real time applications like video and voice overIP. The recommended PHB for this service is the Expedited Forwarding (EF) PHB.
- Platinum, Gold, Silver, and Bronze classes use the Assured Forwarding PHB. These classes are used for real time, delay tolerant traffic and non real time, mission critical traffic.
- Best Effort (standard) class is the standard Internet packet service with an additional, optional use of traffic profiling that is used at the network boundary to request a better effort treatment for packets that are in-profile (packets that do not break the service agreements between the user and the service provider).

Table 165 describes the service classes and the required treatment. Table 166 on page 453 shows how the service classes are mapped to the Business Communications Manager queues.

Table 165 Service classes

Traffic category	Service class	Application type	Required treatment
Critical Network Control	Critical	Critical network control traffic	Highest priority over all other traffic. Guaranteed minimum bandwidth.
Standard Network Control	Network	Standard network control traffic	Priority over user traffic. Guaranteed minimum bandwidth
Real time, delay intolerant, fixed bandwidth	Premium	Person to person communications requiring interaction (such as VoIP).	Absolute bounded priority over user traffic. No packet loss for in-profile traffic. Virtual leased line with lowest amount of latency. Provisioned for peak rate.
Real time, delay tolerant, low variable bandwidth	Platinum	Person to person communications requiring interaction with additional minimal delay (such as low cost VoIP).	Higher-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Real time, delay tolerant, high variable bandwidth	Gold	Single human communication with no interaction (such as Web site streaming video).	High-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, interactive	Silver	Transaction processing (such as Telnet, Web browsing).	Medium priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, non-interactive	Bronze	For example, E-mail, FTP, SNMP.	Lower-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, non-mission critical	Standard	Bulk transfer (such as large FTP transfers, after-hours tape backup).	Best effort delivery. Uses remaining available bandwidth.

Packet classifiers

Filters are organized in groups. A filter group is an ordered list of filters. Each group of filters is associated with actions that are executed when the packet matches the first filter in the group. The filter group and the associated actions constitute a *policy.* A *classifier* is an ordered list of policies. Filters can be added or deleted from an existing group.

The order of a filter group in a classifier is called the group precedence. The lower the order of a group in a classifier the higher the precedence. The order in which filters in a given classifier are evaluated depends on the precedence of the filter group in which the filter resides and, on the order of the filter in the group. Filters in the higher-precedence groups are evaluated before filters in the lower-precedence groups.

A classifier is associated with a role combination. Packets received from any port that has the same role combination are classified with the same classifier. The Policy Table in Unified Manager defines the policies of the classifier associated with a given role combination.

IP filters

IP filters are used to classify IP traffic based on the following criteria:

- Layer 3 information, including IP source and subnet addresses, IP destination and subnet addresses, DSCP, and IP protocols such as TCP/UDP
- Layer 4 information, including TCP/UDP port numbers

Business Communications Manager can use 31 IP filters.

COPS

When used with the Optivity Policy Services® (OPS) Version 1.2 or later, a comprehensive network management application combining IP address management with policy-based network traffic control, Business Communications Manager effectively manages network traffic and resources. Information is transferred using the Common Open Policy Services (COPS) protocol, a query and response protocol that exchanges policy information messages using the Transmission Control Protocol (TCP). Specifically, COPS for Provisioning (COPS-PR) is used to download information. COPS is used to communicate with edge devices on the network.

OPS provides a centralized management point for DiffServ policies. The policy server distributes policies to edge devices and border routers. These edge devices police traffic flows by marking packets and applying forwarding behaviors to the packets at the network node.

For further information about Optivity products, contact your Nortel Networks sales representative.

Policy overview

Use Unified Manager to configure policies and filters to control the behavior of network traffic. A *policy* is a network traffic controlling mechanism that monitors the characteristics of the traffic (for example, its source, destination, and protocol) and performs a controlling action on the traffic when certain user-defined characteristics are matched. A *policy action* is the effect a policy has on network traffic that matches the traffic profile of the policy. You can assign only one action to a policy. You set up *filters* to establish packet-specific criteria that determine how a packet is to be processed. You can use filters to remark packets by updating the DSCP code points, to change priorities, or to drop packets.

LAN ports on Business Communications Manager are configured according to the policy determining traffic priorities. As packets enter the switch, they are marked according to their priority.

After the packets are marked, they are moved to the proper egress queue based on their marking. When a packet is to be transmitted, the switch looks at the Premium queue first. Then Business Communications Manager examines the other queues and sends packets based on the weighted percentage for the queues. The entire process is repeated. This approach ensures that the Premium packets are serviced quickly and that the other data types (other queues) are not starved and serviced in a round-robin fashion.

A packet is processed as follows:

1. The packet enters Business Communications Manager.
2. Filters are applied.
3. Filter actions are taken and the packet can be modified (DSCP).
4. The packet is assigned a QoS class. A QoS class is designated using the DSCP values.
5. The packet is placed in the appropriate egress queue according to its priority marking as described above.
6. The queues are serviced in a round-robin fashion (strict priority or weighted fair queueing).

Implementing Quality of Service (QoS)

The QoS application delivers a set of tools that, when optimally configured, combat escalating bandwidth costs and optimize application performance in your network.

QoS tools allow you to prioritize your critical applications and sensitive traffic. You can tailor appropriate services to support this traffic over the wide area, thus maintaining the necessary performance levels on an end-to-end basis.

Table 166 Default Queue mapping for Business Communications Manager

NNSC	Default DSCP	Business Communications Manager Queue	Business Communications Manager Scheduler
Premium	EF & CS7	0	Strict Priority
Network	CS6	1	Weighted Fair Queuing
Platinum	AF4x	2	Weighted Fair Queuing
Gold	AF3x	3	Weighted Fair Queuing
Silver	AF2x	4	Weighted Fair Queuing
Bronze	AF1x	5	Weighted Fair Queuing
Standard	DE	6	Weighted Fair Queuing

To implement QoS, you need to configure the following:

- QoS Summary parameters
- QoS Devices
- QoS Rules
- QoS Actions
- QoS Policies

Configuring the QoS Summary parameters

The QoS Summary parameters are global settings that affect all of the QoS Policies on your system.

To configure the QoS Summary parameters:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** heading.
   The QoS Summary screen appears.

3 Configure the Summary parameters according to the following table.

Setting	Definition
Description	Shows a description of the QoS service.
Version	Shows the version of the QoS service.
Status	Allows you to enable or disable QoS.
Premium Bandwidth (%)	Enter the percentage of bandwidth to reserve for Premium traffic. You can enter a value from 0% to 90%. **Note**: If you set the Premium Bandwidth too high, you can starve out other traffic.
Video Class	Select the traffic category that is used for H.323 Video traffic. You can assign video traffic as **Premium** or **Best Effort**. **Note**: Choose Best Effort if you want to prevent IP Video traffic from competing with IP Telephony traffic.
Premium DS Code	Enter the DiffServ Code used for Premium traffic on your network. The default value is 0xB8.
Number of Phone Ports	Enter the number of phone ports that are available for QoS. After you change this field, you must reboot the Business Communications Manager system before the change will take affect.

4 Click the **Advanced** tab.
The Advanced screen appears.

5 Click the network adapter you want to modify.

6 On the **Configuration** menu, click **Modify Adapter Water Mark**.
The Advanced property sheet appears.

7 Configure the Advanced parameters according to the following table.

Setting	Definition
Adapter Name	Shows the name of the network adapter you are modifying.
High Water Mark	Enter the High Water Mark for this network adapter. For LAN adapters, you can enter a value from 1 to 37. For WAN and Dialup adapters, you can enter a value from 1 to 5.
Low Water Mark	Enter the Low Water Mark for this network adapter. For LAN adapters, you can enter a value from 1 to 37. For WAN and Dialup adapters, you can enter a value from 1 to 5. **Note**: The value for the Low Water Mark must be lower than the value for the High Water Mark.

8 Click the **Save** button.

9 Repeat steps 5 to 8 for each network adapter you want to modify.

Configuring Devices

The Devices heading provides access to the Interface GroupTable screen, the Interface Queue Table screen, and the DSCP Assignment Table screen. You can configure the Interface Group Table screen. The other two screens provide read-only information.

You view existing interface group configurations, or create or modify an interface group if you want a port (or ports) associated with a role combination for the purpose of assigning the same QoS policy to all interfaces in the group.

Creating an interface group configuration

To create an interface group configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Devices** heading.
   The Interface Group Table screen appears.
3. On the **Configuration** menu, click **Add Interface Group Entry**.
   The Interface Group Table property sheet appears.
4. Configure the Interface Group Table parameters according to the following table.

Attribute	Description
Group Name	Enter the name for the interface group.
Queue Set Id	This is a read only attribute.
Role Combination	Select the interfaces that you want to include in this interface group.
Capabilities	This is a read only attribute.

5. Click the **Save** button.
   The new interface group configuration entry appears in the Interface Group Table.

Modifying an interface group configuration

To modify an Interface group configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QOS** key and click the **Devices** heading.
3. Click the Interface Group Entry you want to change.
4. On the **Configuration** menu, click **Modify Interface Group Entry**.
   The Interface Group Table dialog box opens.
5. Change the Role Combination.
6. Click the **Save** button.

Deleting an interface group configuration

To delete an Interface group configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Devices** heading.
3. Click the Interface Group Entry you want to delete.
4. On the **Configuration** menu, click **Delete Interface Group Entry**.
   A dialog box opens prompting you to confirm your request.
5. Click the **Yes** button.

Configuring Rules

Policy Rules are IP filters that are defined as part of a QoS Policy.

You can create an IP filter, which enables Business Communications Manager to classify traffic. In turn, you can create an access control list from a series of defined filters to create an IP filter group. The filter group then determines access to and denial of network services.

Creating an IP filter configuration

The maximum number of IP filter entries you can add to a QoS Policy is 31.

To create an IP filter configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
   The IP Filter Table screen appears.
3. On the **Configuration** menu, click **Add IP Filter Entry**.
   The IP Filter Table dialog box opens.
4. Configure the IP Filter parameters according to the following table.

Attribute	Description
Name	Enter the name of the IP Filter.
Destination Address	Enter a destination IP address in a valid dot format. This address is used to match the destination IP address in the packet's IP header. If you want to ignore the Destination Address setting for this filter, leave this box blank. If you specify an address in this box, you must also specify a subnet mask in the Destination Mask box.
Destination Address Mask	Enter a mask for the destination IP address in a valid dot format. This address is the destination subnet mask. A subnet mask includes or excludes certain values. Subnetworks (or subnets) extend the IP addressing scheme, allowing you to further divide a network into multiple segments. If you specify a Destination Address, you must also specify a Destination Address Mask. Make sure that the mask and address match with each other. For example, a bitwise AND of the mask and address is equal to the address. If you want to specify a range of addresses, use a subnet mask other than 255.255.255.255. For example, an address/mask combination of 10.10.10.32/255.255.255.252 represents addresses 10.10.10.32-10.10.10.35.

Attribute	Description
Source Address	Enter the source IP address in a valid dot format. This is the IP address to match against the packet's source IP address. If you want to ignore the Source Address setting for this filter, leave this box blank. If you specify an address in this box, you should also specify a subnet mask in the Source Mask box.
Source Address Mask	Enter the source mask of the IP address in a valid dot format. This address is the source subnet mask. A subnet mask includes or excludes certain values. Subnetworks (or subnets) extend the IP addressing scheme, allowing you to further divide a network into multiple segments. If you specify a Source Address, you must also specify a Source Address Mask. Make sure that the mask and address match with each other. For example, a bitwise AND of the mask and address is equal to the address. If you want to specify a range of addresses, use a subnet mask other than 255.255.255.255. For example, an address/mask combination of 10.10.10.32/255.255.255.252 represents addresses 10.10.10.32-10.10.10.35.
DSCP	Enter the DSCP value to match the inbound DSCP. You can enter any decimal value from 0 to 63. If you choose the default (-1), the DSCP value in the packet will be ignored.
Protocol	Select a protocol to match the filter. To select the protocol, choose the protocol from the list or type the numeric value of protocol in the box. You can select TCP, UDP, ICMP, IGMP, RSVP, IP Sec(AH), IPSec(ESP), H323 Video, PPTP, or Match All The default is Match All.
Destination L4 Port	Enter or select a destination port to match the filter. Enter a destination port only if you choose a TCP or a UDP protocol. If you do not want to include the source port in your filter, choose IGNORE. To include a destination port, choose the port from the list services or type the numeric port number of the service. You can choose IGNORE, FTP, TELNET, SMTP, SNMP, DNS, POP, NNTP, or HTTP. You can enter a range of ports by specifying the two limits of the range by a hyphen character, for example, 156-159. You can select all of the ports by entering 0-65536. The default is IGNORE.
Source L4 Port	Enter or select a source port to match the filter. Enter a source port only if you choose a TCP or a UDP protocol. If you do not want to include the source port in your filter, choose IGNORE. To include a source port, choose the port from the list services or type the numeric port number of the service. You can choose IGNORE, FTP, TELNET, SMTP, SNMP, DNS, POP, NNTP, or HTTP. You can enter a range of ports by specifying the two limits of the range by a hyphen character, for example, 156-159. You can select all of the ports by entering 0-65536. The default is IGNORE.
Permit	Select whether packets that match the filter are permitted to pass.

5 Click the **Save** button.

Modifying an IP filter configuration

To modify an IP filter configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
3. Click the entry you want to modify.
4. On the **Configuration** menu, click **Modify IP Filter Entry**.
   The IP Filter Table dialog box opens.
5. Make the changes to the information about the entry.
6. Click the **Save** button.

Deleting an IP filter configuration

To delete an IP filter configuration:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
3. Click the entry you want to delete.
4. On the **Configuration** menu, click **Delete IP Filter Entry**.
   A confirmation dialog box opens.
5. Click the **Yes** button to delete the IP Filter Table entry.

Note: You cannot delete a filter if it is referenced in a filter group.

Creating an IP filter group entry

IP filter groups allow you to assign IP filters to a Policy. An IP filter group can consist of one to several IP filters.

When you create an IP filter group, you choose the IP filters to add and you specify the order in which the IP filters are applied.

The maximum number of IP Filter Group entries you can add to a QoS Policy is 31.

To create an IP filter group table entry:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Rules** heading.
3. Click the **IP Filter Group Table** tab.

4 On the **Configuration** menu, click **Add IP Filter Group Entry**.
The IP Filter Group Table dialog box opens.

5 Configure the IP Filter Group parameters according to the following table.

Attribute	Description
Filter Group Name	Enter the name of the filter group.
Filter Order	Enter the name of the filter to add to the filter group. If you are adding more than one filter, separate the filter names by a comma. The filters are used in the order you specify.

6 Click the **Save** button.

Modifying an IP filter group configuration

To modify an IP filter group configuration:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Rules** heading.

3 Click the **IP Filter Group Table** tab.

4 Click the IP Filter Group you want to modify.

5 On the **Configuration** menu, click **Modify IP Filter Group Entry**.
The IP Filter Group Table dialog box opens.

6 Add or delete filters as a member of the Filter Group. You can also change the order in which the filters are applied.

7 Click the **Save** button.

Deleting an IP filter group entry

To delete an IP filter group entry:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Rules** heading.

3 Click the **IP Filter Group Table** tab.

4 Click the IP Filter Group you want to delete.

5 On the **Configuration** menu, click **Delete IP Filter Group Entry**.
A confirmation dialog box opens.

6 Click the **Yes** button to delete the IP Filter Group Table entry.

Configuring Actions

You configure actions by creating, changing or deleting Actions entries in the Actions screen.

When you assign actions to filters, you specify the type of behavior you want a policy to apply to a flow of IP packets. Actions applied to filters establish packet-specific criteria that determine how a packet is to be processed. You specify the actions associated with specific IP filter groups. When filters match incoming packets, the actions are performed on those packets. Filters can be configured to change the DSCP or to drop packets.

Creating an Action

To create an Action:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Actions** heading.
   The Actions screen appears.
3. On the **Configuration** menu, click **Add Entry**.
   The Actions dialog box opens.
4. Configure the Action parameters according to the following table.

Attribute	Description
Action Name	Enter the name of this Action.
Packet Drop	Select whether this Action drops the packet (**True**) or keeps the packet (**False**). **Note**: If you choose True to drop the packet, you do not need to choose a value for Update DSCP.
Update DSCP	Enter the new DSCP that this Actions assigns to the packet. You can enter a value from -1 to 63. Enter a value of -1 if you do not want this Action to change the DSCP of the packet.

5. Click the **Save** button.

Modifying an Action entry

To modify an action entry:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Actions** heading.
3. Click the entry you want to modify.
4. On the **Configuration** menu, click **Modify Entry**.
   The Actions dialog box opens.
5. Modify the Action parameters.
6. Click the **Save** button.

Deleting an Action Entry

To delete an Action:

1. On the navigation tree, click the **Services** key and the **Policy Management** key.
2. Click the **QoS** key and click the **Actions** heading.
3. Click the Action Entry you want to delete.
4. On the **Configuration** menu, click **Delete Entry**.
   A dialog box opens prompting you to confirm your request.
5. Click the **Yes** button.

Configuring QoS policies

A Policy is an association between Devices (interface groups), Rules (IP filter groups), and Actions. When you create a Policy, you define which Devices are affected, which Rules are checked, and what Actions are taken on the specified interface.

Policies are applied according to the precedence order that you assign in the Policies screen.

Adding a policy

To add a policy:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **QoS** key and click the **Policies** heading.
3. Click the **Add** button.
   Or, right click the **Policies** heading and click **Add**.
   The Add Policies screen appears.
4. Configure the Policy parameters. These parameters are described in the following table.

Attribute	Description
Name	Enter the name of the Policy.
Filter	Select the filter group that is associated with this policy. You must add a filter group, using the Rules heading, before you can choose it from this box.
Filter Type	Shows the type of filter group that is associated with this policy. This is a read only attribute.
Interface Group	Select the Interface group that is associated with this policy. You must add an interface group, using the Devices heading, before you can choose it from this box.
Interface Direction	Shows the direction of packet flow at the interface to which this policy applies. This is a read only attribute.

Attribute	Description
Order	Enter the number used to determine the order of precedence for this policy. Nortel Networks recommends that you consider an order numbering strategy (for the values in the Order field) as you configure policies. The policies in the Policy Table are arranged in ascending order according to value in the Order column. By establishing a policy ordering scheme in multiples of, for example, 10 (Order 10, Order 20, Order 30, Order 40, and so on), you are able to insert policies in the appropriate filter precedence location and still retain the precedence of the remaining policies.
Action	Select the action that is performed with policy. You must add an action, using the Actions heading, before you can choose it from this box.

5 Click the **Save** button.

Modifying a policy

To modify a policy:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Policies** key.

3 Click the heading of the policy you want to modify.

4 Click the policy you want to modify.

5 On the **Configuration** menu, click **Modify Entry**.
The Policy screen appears.

6 Change the Policy attributes.

7 Click the **Save** button.

Deleting a policy

To delete a policy:

1 On the navigation tree, click the **Services** key and click the **Policy Management** key.

2 Click the **QoS** key and click the **Policies** key.

3 Click the heading of the policy you want to delete.

4 Click the **Delete** button.
Or, right click the heading of the policy you want to delete and click **Delete**.
A confirmation dialog box appears.

5 Click the **Yes** button.

Implementing Common Open Policy Services (COPS)

COPS in your networks allows Business Communications Manager to:

- Gather all relevant Policy information from a policy server (COPS).
- Make a decision based on your (as network administrator) set policies and network resources,
- Communicate that decision in the form of proper service to the appropriate group or client (bandwidth, ACLs, QoS).

A solid COPS strategy is closely tied to Internet Protocol (IP) address management and network management. For information about COPS, refer to "COPS" on page 451.

The COPS client options available to you in Unified Manager are:

- Viewing COPS statistics and capabilities
- Creating COPS client configurations

Note: Configure the role combinations before you configuring dynamic policy management (COPS).

Viewing COPS statistics and capabilities

You can view a list of the capabilities of the COPS client and view the COPS objects provided by all of COPS server connections.

To view COPS capabilities and statistics:

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **COPS Client** key and the **Status and Statistics** heading.
   The COPS Client Capability screen appears.

   The COPS Capabilities box displays a list of the COPS protocols supported by Business Communications Manager. The current supported protocol is copsClientVersion1.
3. Click the **COPS Client Status and Statistics** tab.
   The COPS Client Status and Statistics screen appears. All of the information provided on this screen is read only. Table 167 describes the items on this screen.

Table 167 Status page items

Item	Descriptions
Address Type	The type of address in copsClientServerAddress.
Address	The IPv4, IPv6, or DNS address of a COPS server.
Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.

Table 167 Status page items (Continued)

Item	Descriptions
TCP Port	The TCP port number on the COPS server to which the client is connected.
Type	The indicator of the source of the COPS server information. Note: COPS servers can be configured by network management into copsClientServerConfigTable and appear in this entry with type copsServerStatic(1). Alternatively, the type, or entry, can be a notification from another COPS server by way of the COPS PDP-Redirect mechanism and appear as copsServerRedirect(2).
Authorization Type	The indicator of the current security mode in use between the client and the COPS server.
Last Connection Attempt	The timestamp of the last time the client attempted to connect to this COPS server.
State	The operational state of the connection and COPS protocol with respect to this COPS server.
Server Keep Alive Time	The value of the Keepalive timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates no keepalive activity is expected.
Server Accounting Time	The value of the COPS protocol Accounting timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates that the client should not send any unsolicited accounting reports.
In Packets	The total number of COPS packets that the client has received from this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
Out Packets	The total number of COPS packets that the client has sent to this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
In Errors	The total number of COPS packets that the client has received from this COPS server marked for the selected client type that contained errors in syntax. Note: This is a cumulative value and *is not* zeroed on new connections.
Last Errors	The code contained in the last COPS protocol Error Object received by the client from this COPS server marked for the selected client type. Note: This value *is not* zeroed on COPS Client-Open operations.
TCP Connection Attempts	The number of times that the COPS client attempted to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
TCP Connection Failures	The number of times that the COPS client failed to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
Open Attempts	The number of times that the COPS client attempted to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
Open Failures	The number of times that the COPS client failed to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.

Table 167 Status page items (Continued)

Item	Descriptions
Unsupported Client Type	The total number of COPS packets that this client has received from COPS servers that referred to client types that are unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Unsupported Version	The total number of COPS packets that this client has received from COPS servers marked for the selected client type that had a COPS protocol version number that is unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Length Mismatch	The total number of COPS packets that the client received from COPS servers marked for the selected client type that had a COPS protocol message length that did not match the actual received packet. Note: This is a cumulative value and *is not* zeroed on new connections.
Unknown Opcode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Unknown Cnum	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Num not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Bad Ctype	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Type not defined for the C-Nums known by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Bad Sends	The total number of COPS packets that the client attempted to send to COPS servers marked for the selected client type that resulted in a transmit error. Note: This is a cumulative value and *is not* zeroed on new connections.
Wrong Objects	The total number of COPS packets that the client received from COPS servers marked for the selected client type not containing a permitted set of COPS protocol objects. Note: This is a cumulative value and *is not* zeroed on new connections.
Wrong OpCode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code that should not have been sent to a COPS client, for example, Open-Requests. Note: This is a cumulative value and *is not* zeroed on new connections.
Timeout Clients	The total number of times that the client has been shut down for the selected client type by COPS servers that detected a COPS protocol Keepalive timeout. Note: This is a cumulative value and *is not* zeroed on new connections.
Auth Failures	The total number of times that the client received a COPS packet marked for the selected client type that could not be authenticated using the authentication mechanism used by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
Auth Missing	The total number of times that the client received a COPS packet marked for this client type not containing authentication information.

Configuring a COPS Client

To Configure a COPS client, you enter the information the COPS Client needs to connect to a COPS Server.

Adding a COPS Client Server entry

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **COPS Client** key and the **Configuration** heading.
   The COPS Client Server screen appears.
3. On the **Configuration** menu, click **Add Cops Client Config Entry**.
   The COPS Client Server screen appears.
4. Configure the COPS Client Server parameters according to the following table.

Attribute	Description
Address Type	Shows the type of address used for this COPS Client server.
Address	Enter the IP address of the COPS Client server in a valid dot format.
Client Type	Displays the COPS Client type the server is capable of serving.
Authorization Type	Displays the Authorization type used for the server.
TCP Port	Displays the TCP Port used to communicate with the COPS server.
Priority	The Priority determines the order in which the COPS Client attempts to connect to the COPS Server. The COPS Client attempts to connect to the COPS Server with the highest number first. You can enter a value from 0 to 65535. **Note**: If you enter the same Priority for two COPS Servers, the COPS client will randomly select which COPS server to try first.

5. Click the **Save** button.

Modifying a COPS Client Server entry

The TCP Port and Priority are the only parameters you can modify on a COPS Client Server entry.

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **COPS Client** key and the **Configuration** heading.
   The COPS Client Server screen appears.
3. Click the COPS Client Server entry you want to modify.
4. On the **Configuration** menu, click **Modify Cops Client Config Entry**.
   The COPS Client Server screen appears.
5. Change the TCP Port or Priority of the COPS Client server.
6. Click the **Save** button.

Modifying the COPS Client Server Retry Data

If Business Communications Manager cannot connect to the COPS Client Server on its first attempt, Business Communications Manager will wait and then try to connect again. On the COPS Client Server Retry Data screen, you can enter the number of times that Business Communications Manager attempts to connect again and time it waits between attempts.

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **COPS Client** key and the **Configuration** heading.
   The COPS Client Server screen appears.
3. Click the **COPS Client Server Retry Data** tab.
   The COPS Client Server Retry Data screen appears.
4. Configure the COPS Client Server Retry Data according to the following table.

Attribute	Description
Server Retry Count	Enter the number of times that Business Communications Manager attempts to connect to the COPS Server if the original connection attempt fails. You can enter a value from 0 to 9999 attempts.
Server Retry Interval	Enter the amount of time that Business Communications Manager waits before attempting to connect to the COPS Client Server again. You can enter a value of 0 to 65535 centiseconds. Note: 100 centiseconds equals one second.

5. Press the **Tab** key to save your changes.

Configuring the Policy Agent characteristics

You can configure the Policy Agent operational parameters. To configure a Policy Agent.

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **Policy Agent** heading.
   The Policy Service screen appears.
3. Configure the Policy Service settings according to the following table.

Attribute	Description
Description	Shows a description of the Policy Agent Service.
Version	Shows the version number of the Policy Agent Service.
Status	Shows the status of Policy Agent Service. This box also provides commands to enable or disable the Policy Agent Service. Possible values: **Up**, **Disabled**, **Enabled** The default value is **Up**.

4. Press the **Tab** key to save your settings.
5. Click the **Policy Agent** tab.
   The Policy Agent screen appears.
6. Configure the Policy Agent settings according to the following table.

Attribute	Description
Dynamic Management	Allows you to enable or disable the Policy Server Control. The default value is Disabled. **Note**: If you enable Dynamic Management, local policy control is disabled.
Policy Agent State	Shows the current status of the policy Agent. The possible states are: Running, Initializing or Disabled.
Policy Agent Retry Timer	Enter the time, in seconds, between the receipt of a connections termination/rejection indication and the start of a new connection request. You can enter -1 or a value between 1 and 86400. Note: If you enter a value of -1, a connection retry is not attempted after a failed attempt.

7. Press the **Tab** key to save your settings.
8. Click the **Policy Server** tab.
   The Policy Server screen appears.
9. Configure the Policy Server settings according to the following table.

Attribute	Description
Name	Shows the name of the Policy Server.
ID	Shows the ID of the Policy Server.

Attribute	Description
Longevity	Allows you to specify when the policy received from the Policy Server expires. The possible values are: **Never Expire**, **Expire Immediately**, **Expire on Timeout** The default value is: **Expire Immediately**.
Time to Live	If you chose Expire on Timeout in the Longevity box, enter the timeout in this box. You can enter a value between 0 and 65535 seconds.

10 Press the **Tab** key to save your settings.

11 Click the **Policy Class Support Table** tab.
The Policy Class Support Table screen appears.

12 This screen displays read only information. This information is described in the following table.

Attribute	Description
Policy Name	Shows the name of the policy.
Current Instances	Shows the current class entries.
Maximum Installed Instances	Shows the maximum number of allowed class entries.

13 Click the **Policy Device Identification** tab.
The Policy Device Identification screen appears.

14 This screen displays read only information. This information is described in the following table.

Attribute	Description
Description	Shows a description of the Business Communications Manager system.
Maximum Message Size	Shows the maximum target message size supported by Business Communications Manager. The maximum COPS message size is 2048.

15 Press the **Tab** key to save your settings.

IP Firewall Filters

The Business Communications Manager IP Firewall Filters feature is one of the security features Business Communications Manager offers to protect your network against intruders. The security and firewall features are also used for controlling what outside resources your users will be able to access. The following features are part of the Business Communications Manager firewall:

- Basic (stateless) Packet Filter
- Stateful Packet Filters

Caution: When blocking incoming packets, make sure you do not block your access to Unified Manager on the system.

Note: For information on using filters for IPX routing, see "IPX Routing" on page 384.

Packet filtering

A packet filter is a firewall facility that inspects incoming and outgoing packets and uses this information to determine which network packets to allow through the firewall. The traffic may or may not be tracked by keeping the state of the connection.

Basic (stateless) Packet Filter

Business Communications Manager supports basic (or stateless) packet filtering for IP protocols. Stateless packet filtering examines each packet and determines whether or not to pass it through based on the rules entered. No state is maintained for packets evaluated using stateless rules.

Basic Packet Filters are configured by setting the **Stateful** box on the interface screen to No.

Stateful Packet Filters

Business Communications Manager supports stateful packet filtering for IP protocols. Stateful packet filters monitor active sessions and record session information such as IP addresses and port numbers. They maintain state information for each flow (TCP, UDP or ICMP). Stateful filters use the state information to determine if a packet is responding to an earlier request that has been validated by the rule set. If the packet is in response to a previous request, the packet is treated in the same manner. It will either be blocked or allowed though.

Stateful packet filters protect your network against Internet attacks such as source spoofing, where an attacker pretends to be a trusted user by using an IP address that is within the accepted range of IP addresses of your internal network. Business Communications Manager stateful packet filtering validates that addresses coming from outside the network are valid outside addresses. Stateful packet filters also protect your network from a denial-of-service attack, where an attacker tries to block valid users from accessing a resource or a server.

Stateful filtering supports TCP, UDP, IP, and ICMP. Stateful filtering supports the following applications: H.323, FTP, HTTP, POP3, Telnet, SMTP, DNS, DHCP, TFTP, GOPHER, FINGER, NNTP, NetBios, POP2, RPC, SNMP and SUNNFS.

IP Firewall filters and NAT

When you use NAT and IP Firewall filters, there are two interactions you need to be aware of.

- On inbound traffic, the NAT rules are applied before the IP Firewall Filter rules.
- On outbound traffic, the IP Firewall Filter rules are applied before theNAT rules.

Viewing and changing the status of Firewall Filters

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **IP Firewall Filters** heading.
   The Firewall Filters Summary screen appears. The Summary screen attributes are:

Attribute	Description
Description	Shows a description of Firewall Filters.
Version	Shows the version number of the subsystem.
Status	Shows the status of Firewall Filters. This box also provides commands to enable or disable Firewall Filters. Possible values: **Disabled**, **Enabled** When the status is Enabled, the state of all of the traffic is monitored. Rules can then be set for each of the interfaces, as necessary. The default value is: **Disabled**

3. Press the **Tab** key to save your settings.

Configuring IP Firewall Filters for an interface

Note: This section describes configuring IP Firewall Filters for a single interface. Follow the same instructions to configure the parameters for each of the other interfaces.

The following procedures describe how to configure a single interface (LAN1 for example).

1. On the navigation tree, click the **Services** key and click the **Policy Management** key.
2. Click the **IP Firewall Filters** key and click the heading of the interface you want to configure.
   The Logging Settings screen appears.
3. Click the **Logging** box and click **Disabled** or **Enabled**.

4 Click the **Logging Level** box and click one of the following options:
- Level **1** logs errors only
- Level **2** logs warnings
- Level **3** logs everything

5 Press the **Tab** key to save your settings.

6 Click the **Log Viewing Options** tab.
The Log Viewing Options screen appears.

7 Enter the **Start Date** and **End Date** (mm/dd/yyyy).
This is necessary only if you wish to view existing logging data.

Note: You can configure rules several ways; using default rules, setting up individual rules, or a combination of the two.

Adding Default Rules

Caution: If you turn on the Default Rules, you cannot access Unified Manager on this interface.

1 Click the **Default Rule Status** tab.
The Default Rule Status screen appears.

2 Click the **Status** box and click one of the following options:

- **Enabled - Pass Outgoing and Block Incoming Except IP Phones**
  Allows IP telephony traffic through, but blocks all other traffic on this interface.
- **Enabled - Pass Outgoing and Block Incoming Including IP Phones**
  Blocks all traffic on this interface, including IP telephony traffic.
- **Disabled - Pass All**
  The IP Firewall does not check the traffic on this interface. Therefore, all traffic on this interface, both incoming and outgoing, is passed through.

The default is **Disabled**.

Note: Setting an Incoming Rule that blocks all incoming packets and disabling the Default Rules is not the same as enabling the Default Rules.

When block all incoming packets and disable the Default Rules, packets that originate from inside the Firewall are not treated as Stateful. When a response packet is returned, it will not match the Incoming Rule and will be blocked.

When you enable the Default Rules, packets that originate from inside the Firewall are treated as Stateful. When a response packet is returned, it will match the existing state and will be passed.

Adding an Input Filter for a Firewall Filter Interface

Before you can specify a Rule Order, you must add Filter Rules.

The maximum number of Input Filter Rules you can add is 32.

1 Click the **Input Filters' Rule Settings** tab.
The Input Filters' Rule Settings screen appears.

2 On the **Configuration** menu, click **Add Input Filter Rule**.

3 Configure the Input Filter Rule settings. These settings are described in the following table:

Attribute	Description
Rule Name (IR# or OR#)	Allows you to assign a number to the Rule.
Stateful	Allows you to specify if the states of connections that match this rule will be monitored. This permits the creation of one-way rules. For example, you can permit inside traffic to return but block traffic originating from the outside. For more information refer to "Stateful Packet Filters" on page 470. The values are **Yes** and **No**. The default is **Yes**.
Disposition	Allows you to specify if a packet that matches this rule passes through or is blocked. The values are **Block** or **Pass**. The default is **Block**.
Protocol	Allows you to specify the protocol type of the packet to be filtered. The values are; **IP**, **TCP**, **UDP**, **TCP/UDP** and **ICMP**. The default is **IP**.
Source IP Type	Allows you to specify if the Source IP is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Source IP and Source IP Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Source IP	Allows you to specify the source address of the packet to be filtered.
Source Range Mask	Allows you to specify the source address mask of the packet to be filtered. If you enter 255.255.255.255, then the Source IP is a single address. If you enter 0.0.0.0, then the Source IP is all possible addresses.
Source Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following: **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **DNS**, **DHCP**, **TFTP**, **Gopher**, **Finger**, **HTTP**, **H.323**, **POP**, **NNTP**, **NetBios**, **RPC**, **SUNNFS** and **DCOM**.
Destination IP Type	Allows you to specify if the Destination IP Type is **Fixed** or **Dynamic**. Use Dynamic when the IP is assigned by an outside source. For example, your Internet Service Provider (ISP) assigns your IP address. If you specify Dynamic, Destination IP and Destination IP Mask do not need to be entered. The default is **Fixed**. **Note**: Dynamic does not match all IP addresses. If you want to match all IP addresses, enter an IP address of 0.0.0.0 and a mask of 0.0.0.0.
Destination IP	Allows you to specify the Destination IP address.

Attribute	Description
Destination Range Mask	Allows you to specify the destination address mask of the packet to be filtered. If you enter 255.255.255.255, then the Destination IP is a single address. If you enter 0.0.0.0 then the Destination IP is all possible addresses.
Destination Port Range (#-#)	Allows you to specify a single entry, a range of entries (1-65535) or one of the following: **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **DNS**, **DHCP**, **TFTP**, **Gopher**, **Finger**, **HTTP**, **POP**, **NNTP**, **NetBios**, **RPC**, **SUNNFS** and **DCOM**.
Source Routing	Allows you to specify how the Source Routing is checked. **Allow**: Rule matches Only if the packet has the source routing option set. **Deny**: Rule matches Only if the packets does not have the source routing option set. **Ignore**: The source routing option in the packet is not checked and therefore all packets will match. The default is **Ignore**.
IP Options	Allows you to specify how the IP Options are checked. **Allow**: Rule matches Only if the packet has the IP options set. **Deny**: Rule matches Only if the packets does not have the IP options set. **Ignore**: The IP Options in the packet are not checked and therefore all packets will match. The default is **Ignore**.
Quick	Allows you to specify the order of rule match. Yes means that the first rule match is used. No means the last rule match is used. The default is Yes.

Note: When you set filters, make sure you allow the flow of packets going to the RPC port (port 135 TCP or UDP), DCOM ports, and the Unified Manager port (port 6800 TCP) for correct Unified Manager operation. For more information about allowing Unified Manager access, refer to "Accessing Unified Manager through the Firewall" on page 476.

4 Click the **Save** button.

Modifying an Input Filter for a Firewall Filter Interface

1 Click the **Input Filters' Rule Settings** tab.
The Input Filters' Rule Settings screen appears.

2 Click the Input Filter you want to modify.

3 On the **Configuration** menu, click **Modify Input Filter Rule**.

4 Modify the Input Filter Rule attributes.

5 Click the **Save** button.

Deleting an Input Filter for a Firewall Filter Interface

1. Click the **Input Filters' Rule Settings** tab.
   The Input Filters' Rule Settings screen appears.
2. Click the Input Filter you want to delete.
3. On the **Configuration** menu, click **Delete Input Filter Rule**.
   A message appears that asks you to confirm the deletion.
4. Click the **Yes** button.

Configuring the order of the Input Filters for an interface

After you enter all of the Input filters, you need to set the order in which the filters are used.

1. Click the **Input Rules' Filter Order** tab.
   The Input Rules' Filter Settings screen appears.
2. Type in the Input Filters' Rule Order for the interface you are configuring.
3. Press the **Tab** key to save your settings.

Adding an Output Filter for a Firewall Filter Interface

Before you can specify a Rule Order, you must add Filters.

The maximum number of Output Filter Rules you can add is 32.

1. Click the **Output Filter Rules' Setting** tab.
   The Output Filter Rules' Settings screen appears.
2. On the **Configuration** menu, click **Add Output Filter Rule**.
3. Configure the Output Filter Rule settings. These setting are described in the table in "Adding an Input Filter for a Firewall Filter Interface" on page 473.
4. Click the **Save** button.

Modifying an Output Filter for a Firewall Filter Interface

1. Click the **Output Filter Rules' Setting** tab.
   The Output Filter Rules' Settings screen appears.
2. Click the Output Filter you want to modify.
3. On the **Configuration** menu, click **Modify Output Filter Rule**.
4. Modify the Output Filter attributes.
5. Click the **Save** button.

Deleting an Output Filter for a Firewall Filter Interface

1. Click the **Output Filter Rules' Setting** tab.
   The Output Filter Rules' Settings screen appears.
2. Click the Output Filter you want to delete.
3. On the **Configuration** menu, click **Delete Output Filter Rule**.
   A message appears that asks you to confirm the deletion.
4. Click the **Yes** button.

Configuring the order of the Output Filters for an interface

After you enter all of the Output filters, you need to set the order in which the filters are used.

1. Click the **Output Filter Rules' Order** tab.
   The Output Filter Rules' Configuration screen appears.
2. Type in the Output Filters' Rule Order for the interface you are configuring.
3. Press the **Tab** key to save your settings.

Accessing Unified Manager through the Firewall

- Do not set any blocking input rules on the interface that you use to connect to Business Communications Manager using Unified Manager. This includes enabling the default rules.
- Set three Input Rules for Unified Manager traffic, one for RPC, one for DCOM and one for port 6800. Configure these three rules as follows:

Table 168 Input Rule Configuration for Unified Manager — RPC

Direction:	In
Protocol:	TCP/UDP
Destination IP Type:	Fixed (or Dynamic if the IP address is remotely assigned)
Destination IP:	IP address for this interface (or blank if IP Type is Dynamic)
Destination IP Mask:	Appropriate mask (or blank if IP Type is Dynamic)
Destination Port Range:	RPC
Source IP Type	Fixed
Source IP	IP address of the system that will access Business Communications Manager
Source IP Mask:	255.255.255.255 (or as appropriate)
Source Port Range:	ALL

Table 169 Input Rule Configuration for Unified Manager — DCOM

Direction:	In
Protocol:	TCP/UDP
Destination IP Type:	Fixed (or Dynamic if the IP address is remotely assigned)
Destination IP:	IP address for this interface (or blank if IP Type is Dynamic)
Destination IP Mask:	Appropriate mask (or blank if IP Type is Dynamic)
Destination Port Range:	DCOM
Source IP Type	Fixed
Source IP	IP address of the system that will access Business Communications Manager
Source IP Mask:	255.255.255.255 (or as appropriate)
Source Port Range:	ALL

Table 170 Input Rule Configuration for Unified Manager — port 6800

Direction:	In
Protocol:	TCP/UDP
Destination IP Type:	Fixed (or Dynamic if the IP address is remotely assigned)
Destination IP:	IP address for this interface (or blank if IP Type is Dynamic)
Destination IP Mask:	Appropriate mask (or blank if IP Type is Dynamic)
Destination Port Range:	6800
Source IP Type	Fixed
Source IP	IP address of the system that will access Business Communications Manager
Source IP Mask:	255.255.255.255 (or as appropriate)
Source Port Range:	ALL

Note: The order of these three rules does not matter, as long as these rules come before more general rules.

Chapter 20
Configuring Management Settings

The following shows the programming map for **Management**:

In Unified Manager, **Management** allows you to manage user and alarm settings. Under the **Management** heading, Unified Manager displays the following subheadings:

- **User Manager”** displays the User Profile window showing a list of the current user name and associated passwords and access privileges. The User Profile window allows you to add, modify or delete any user profile information.
- **Alarm Manager**” displays the Alarm Database, SNMP Trap and the Alarm Backup Batch Job windows. The Alarm Database window allows you to modify event information collection parameters. The SNMP Trap window allows you to enable or disable the sending of different SNMP traps. The Alarm Backup Batch Job window allows you to enable or disable and to schedule alarm backup batch job.

User Manager

Business Communications Manager comes with the following default user profiles:

- **manager**: Default password: “Manager”. Access privilege: Read-Write
- ModemBackup (North America only):
- **supervisor**: Default password: “visor”. Access privilege: Administrator
- **user**: read-only type user, with “User” as the default password

Note: After installation, change the administrator type passwords.

Warning:

The ModemBackup password, must match the password required by the far end of the connection. If this password does not match to the far end requirement, Business Communications Manager cannot make a dialup network connection if NetLinkManager detects a break in the permanent link.

Adding a user profile

To add a user profile:

1. Select **Management, User Manager**.
   The User Profile screen appears showing the current user profile information.
2. From the **Configuration** menu, select **Add User**.
   The User Profile dialog box appears.
3. Use the following table to add the new user profile information:

Attribute	Description
User Name	Allows you to enter the user name. The User Name is case-sensitive and must not exceed 50 characters in length.
Password	Allows you to assign a password for the user. The password is case-sensitive and must exceed 15 characters in length.
Confirmed Password	Allows you to enter the password again to validate the new or modified password.
Privilege	Allows you to select the level of access associated with the user name. The following levels of access are available: READ-ONLY: Allows you to view programming settings, but not to modify them. READ-WRITE: Allows you to view and modify programming settings. READ-WRITE-DIAL: Allows you to view, modify and use a network dial-up connection. READ-ONLY-CDR: Allows you to view CDR programming settings. READ-WRITE-CDR: Allows you to view and modify CDR programming settings.

4. Click the **SAVE** button to save your settings.
   The new user profile information is added to the list on the User Profile window.

Modifying a user profile

To modify a user profile:

1. Select **Management, User Manager**.
   The User Profile window appears showing a list of the current user profiles.
2. Click the User Name for the user profile you want to modify.
   The row containing that user profile information is highlighted.
3. From the **Configuration** menu, select **Modify User**.
   The User Profile dialog box appears.

Note: You cannot modify a user name. You must delete the complete User Profile row from the User Profile window and add a profile with the new name.

4. Make the necessary changes in the User Profile dialog box.
5. Click the **SAVE** button to save your settings.

Deleting a user profile

To delete a user profile:

1. Select **Management, User Manager**.
   The User Profile window appears showing a list of the current user profiles.
2. Click the User Name you want to delete.
   The row containing the user profile information is highlighted.
3. From the **Configuration** menu, select **Delete User**.
4. Click the **YES** button to delete the user profile.

Note: Maintain only one user profile with administrator privileges and allow only the system administrator to use this user profile. Multiple users logging on to Business Communications Manager from different client stations using the administrator account can cause inconsistent or wrong configuration.

Alarm Manager

The Alarm Manager enables you to manage the collection and storage of alarm information. The Alarm Manager allows you to set different collection parameters for the Alarm Database. You can use the Alarm Manager to enable or disable the sending of all or some types of SNMP traps. The Alarm Manager provides the Alarm Backup Batch Job, an application which backs up old alarm records to an archive folder at a scheduled time.

Business Communications Manager provides real-time information about what is occurring within the Business Communications Manager system through the Alarm Banner and the Alarm Browser.

The Business Communications Manager alarm system includes the following components:

- Alarm Banner: The Alarm Banner provides a window which allows you to continually monitor the Business Communications Manager system for alarms. For more information, see “Fault Alarm Banner” on page 535.
- Alarm Browser: The Alarm Browser allows you to browse through a list of alarms and provides detailed information on each one. For more information, see “Alarm Browser” on page 536.

Configuring the Alarm Manager

1. On the navigation tree, click the **Management** key and click **Alarm Manager**. The Alarm Database, SNMP Trap and Alarm Backup Batch Job windows appear.
2. Use the following table to configure the Alarm Database:

Attribute	Description
Maximum Number Record	Allows you to set the maximum number of records that the alarm database stores. The default is 0 (no limit). The range is from 0 to 5000.
Kept Timer (days)	Allows you to set the number of days that the records remain in the database before the record is archived.
Resync Timer (seconds)	Allows you to set, in seconds, the interval at which the alarm service synchronizes with the Windows NT event logs.
Archive Location	Allows you to enter the path to the directory where the archives of alarm information is kept. The default path is: d:datafiles\nortel networks\unified manager\archive\ An archive of the alarm information is made when an Alarm Backup Batch Job is run or when Business Communications Manager is rebooted (if the Alarm Service is running). The Business Communications Manager logs are emptied when the logs are archived. The file names of the Business Communications Manager log archives are: • System Log SystemLogYYMMDDHHMM.evs • Administration Log ApplicationLogYYMMDDHHMM.evs • Information Log SecurityLogYYMMDDHHMM.evs Where: • YY is the year the archive was created • MM is the month the archive was created • DD is the day the archive was created • HH is hour the archive was created • MM is the minute the archive was created

3. Press the **TAB** key to save your settings.
4. Use the following table to configure the SNMP Trap:

Attribute	Description
TrapsEnabled	Allows you to enable or disable the sending of SNMP traps when a new event arrives in the alarm database.
EventInfo Enabled	Allows you to enable or disable sending SNMP traps when an “Information” event arrives in the alarm database.
EventWarning Enabled	Allows you to enable or disable sending SNMP traps when a “Warning” event arrives in the alarm database.
EventError Enabled	Allows you to enable or disable sending SNMP traps when an “Error” event arrives in the alarm database.
SrcExclusion List	Allows you to add, in a comma-separated format, a list of event sources from which SNMP traps must not be generated. The source exclusion list prevents you from receiving SNMP traps which have no meaning to you.

5 Press the **TAB** key to save your settings.

6 Use the following table to configure the Alarm Backup Batch Job:

Attribute	Description
Batch Job	Allows you to start or stop a scheduled batch backup to an archive folder. The Alarm Backup Batch Job uses the Kept Timer value from the Alarm Database screen to determine when to archive an alarm record.
Schedule Day	Allows you to set the day when the system must perform the backup.
Schedule Time	Allows you to set the time the backup must start.

Tips

Before you change the day or time, or both, you must first stop the batch job, make your changes, and then start the batch job again.

7 Press the **TAB** key to save your settings.

Chapter 21
Backup and Restore Utility (BRU)

This chapter describes how to use the Backup and Restore Utility (BRU). With BRU you can:

- Backup the Business Communications Manager settings
- Restore the Business Communications Manager settings
- Schedule a Backup
- Administer the backup volumes
- Save a Backup job
- Transfer files

Starting BRU

To start BRU:

1. Launch your web browser.
2. In the URL address field, type the Business Communications Manager IP address and add port 6800.
   For example: HTTP://10.10.10.1:6800
   The Unified Manager initial page appears.

   Note: You must include HTTP:// to access Unified Manager.

3. Click the **BRU** button.
4. In the **User Name** box, type the administrator user name.
   The default administrator user name is **supervisor**.
5. In the **Password** box, type the administrator password.
   The default administrator password is **visor**.

   Note: If you have changed the default administrator user name and password, use the new user name and password in steps 4 and 5. For information about how to change a user name and password, refer to “Modifying a user profile” on page 480.

6. Click the **OK** button.
   The BRU screen appears

Backing up Business Communications Manager settings

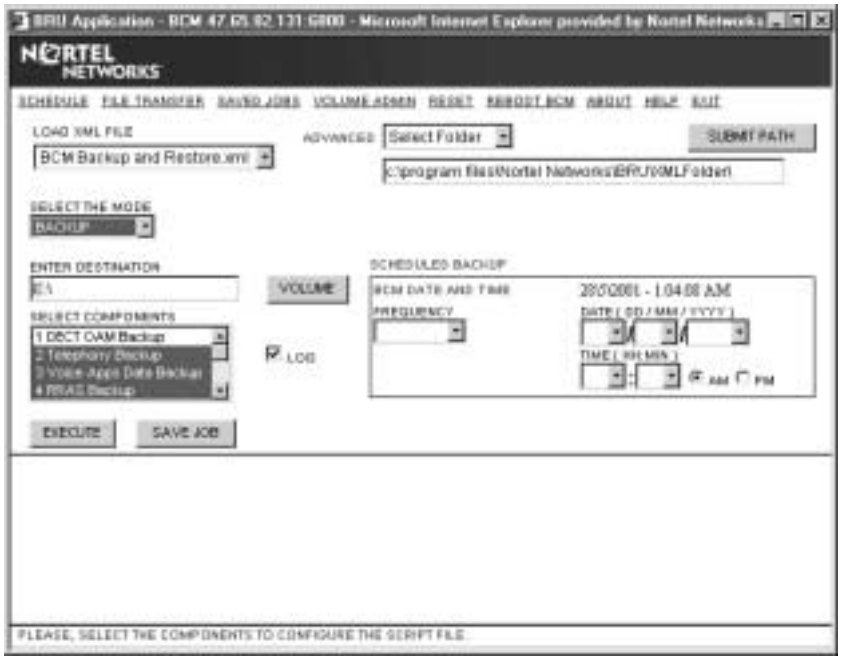
A backup saves your Business Communications Manager settings to a volume on the Business Communications Manager system or another computer on the network. In the unlikely event that your Business Communications Manager loses its settings, you can restore the backed up settings to your Business Communications Manager system.

Note: Nortel Networks recommends that you backup Business Communications Manager on a regular basis.

1 Start BRU.
The BRU screen appears

2 From the **Load XML File** list box, select **BCM Backup and Restore.xml**.
The Select the Mode list box appears.

3 From the **Select the Mode** list box, select **BACKUP**.
The BRU screen changes and displays the backup options.



4 Click the **Volume** button.
The Volume Administration screen appears.

5 Click the **Select** button beside the volume in which you want to store the backup.
If you want to store the backup in a volume that does not appear on the list, refer to "Adding volumes" on page 491 for information on how to add volumes.

6 From the **Select Components** list, select the components you want to back up.
By default, all of the components except DECT OAM are selected.

7 Click the **Execute** button to run the backup job.
The User Name and Password screen appears.
Note: If you are backing up the file to a Local volume, the User Name and Password screen does not appear. Go to step 11.

8 In the **Username** box, type the user name required to access the remote volume.
Use a domain name qualifier if you are required to.

9 In the **Password** box, type the password required to access the remote volume.

10 Click the **Submit** button.
The Report File Name screen.

11 In the **Report File Name** box, type a name for the report for this backup job.
This report contains the results of the backup process and is stored in the same folder as the backup.

12 Click the **Submit** button.

13 If you chose to backup the DECT OAM component, the DECT OAM Password screen appears. In the **Password** box, type the DECT OAM Installer password and click the **Submit** button. The default DECT OAM Installer password is **insta**.

14 When the backup is finished, a dialog box appears.
If the dialog box confirms the backup was successful, click the **OK** button.
If the dialog box indicates an error, click the **OK** button and check the log file for errors. Correct the cause of the errors and try the backup again.

Restoring Business Communications Manager settings

A restore copies the Business Communications Manager settings from a backup volume to the Business Communications Manager system.

The Business Communications Manager system must be operational and you must be able to access it using Unified Manager before you can restore the settings. For example, if a component on your Business Communications Manager system was replaced and all of the programming was set to default, you would have to perform the Initialization procedure described in the *Business Communications Manager Installation and Maintenance Guide* before you could perform the restore.

Note: If the repair to your Business Communications Manager system included replacing the MSC, you must get and install new software keycodes before you can restore the settings. Your old software keycodes will not work with the new MSC.

Note: If you restore programming to a different system than the system from which the backup was created, you must set the time zone on the restored system using Unified Manager.

1 Start BRU.
The BRU screen appears

2 From the **Select XML File** list box, select **BCM Backup and Restore.xml**.

3 From the **Select the Mode** list box, select **Restore**.
The BRU screen displays the restore options.

4 Click the **Volume** button.
The Volume Administration screen appears.

5 Click the **Select** button beside the volume you want to use to restore the settings.

6 From the **Select Components** list box, select the components you want to restore.
The components that are backed up appear highlighted in the list.

7 Click the **Execute** button.
The User Name and Password screen appears.
Note: If you are backing up the file to a Local volume, the User Name and Password screen does not appear. Go to step 11.

8 In the **Username** box, type the user name required to access the remote volume.
Use a domain name qualifier if you are required to.

9 In the **Password** box, type the password required to access the remote volume.

10 Click the **Submit** button.

11 In the **Report File Name** box, type a name for the report for this backup job.
This report contains the results of the restore process and is stored in the same folder as the backup.

12 Click the **Submit** button.

13 When the restore is finished, a dialog box appears.
If the dialog box confirms the restore was successful, click the **OK** button.
If the dialog box indicates an error, click the **OK** button and check the log file for errors. Correct the cause of the errors and try the restore again.

14 A dialog box appears, indicating you need to reboot Business Communications Manager.
Click the **OK** button to reboot Business Communications Manager.

Scheduling a backup

You can schedule a backup to start at a later time or date. This allows you to run the backup at a more convenient time or when there is less network traffic.

You can also schedule the backup to repeat on a regular basis. Nortel Networks recommends that you do backups on a regular basis to capture new changes to theBusiness Communications Manager settings and data.

1 Start BRU.
The BRU screen appears

2 From the **Select XML File** list box, select **BCM Backup and Restore.xml**.

3 From the **Select the Mode** list box, select **BACKUP**.
The BRU screen changes and displays the backup options.

4 Click the **Volume** button.
The Volume Administration screen appears.

5 Click the **Select** button beside the volume in which you want to store the backup.
If you want to store the backup in a volume that does not appear on the list, refer to "Adding volumes" on page 491 for information on how to add volumes.

6 From the **Select Components** list, select the components you want to back up.
By default, all of the components except DECT OAM are selected.

7 In the **Frequency** list box, select how often this scheduled backup will run.
Select **Once** to run this backup one time at the time and date specified.
Select **Daily** to run this backup every day at the time specified.
Select **Weekly** to run this backup on the same day and time every week (for example, Monday at 4:00 am).
Select **Monthly** to run this backup on the same date and time every month (for example, the 15 of the month at 4:00 am).

8. In the three **Date** list boxes, enter the day, month and year when you want this backup to run. If you chose Daily, Weekly or Monthly for the Frequency, this is the date when the first backup runs.
9. In the two **Time** list boxes, enter the hours and minutes when you want this backup to run. Click the **AM** or **PM** option.
   If you chose Daily, Weekly or Monthly for the Frequency, this is the time when all of the subsequent backup will run.
10. Click the **Execute** button.
    The User Name and Password screen appears.
    Note: If you are backing up the file to a Local volume, the User Name and Password screen does not appear. Go to step 15.
11. In the **Username** box, type the user name required to access the remote volume.
    Use a domain name qualifier if you are required to.
12. In the **Password** box, type the password required to access the remote volume.
13. Click the **Submit** button.
    The Report File Name screen.
14. In the **Report File Name** box type a name for the report for this backup job.
    This report contains the results of the backup process and is stored in the same folder as the backup.
15. Click the **Submit** button.
16. If you chose to backup the DECT OAM component, the DECT OAM Password screen appears. In the **Password** box, type the DECT OAM Installer password and click the **Submit** button. The default DECT OAM Installer password is **insta**.

The backup job is scheduled.

Viewing the scheduled backups

1. Start BRU.
   The BRU screen appears
2. Click the **Schedule** link.
   The Scheduled Backups screen appears. All of the backups scheduled for this Business Communications Manager appear on this screen.
3. Click the **Close** button to close the Scheduled Backups screen.

Viewing a scheduled backup report

1. Start BRU.
   The BRU screen appears
2. Click the **Schedule** link.
   The Scheduled Backups screen appears. All of the backups scheduled for this BCM appear on this screen.
3. Click the **View Report File** link beside the scheduled backup.
4. To view the report on your computer, click the **Open this file from its current location** option.
   To save the report on your computer, click the **Save this file to disk** option.
5. Click the **Close** button to close the Scheduled Backups screen.

Deleting a scheduled backup

1. Start BRU.
   The BRU screen appears
2. Click the **Schedule** link.
   The Scheduled Backups screen appears.
3. Click the **Delete** button beside the scheduled backup you want to delete.

Administering backup volumes

Backup volumes are the locations where you store the backed up settings.You administer the backups volumes from the Volume Administration screen. From this screen you can:

- add volumes
- modify volumes
- delete volumes.

Adding volumes

1. Start BRU.
   The BRU screen appears.
2. Click the **Volume Admin** menu.
   The Volume Administration screen appears.
3. In the **Status** list box, click **Local** or **Remote**.
   Click **Local** if you want the backup stored in a volume on the Business Communications Manager.
   Click **Remote** if you want the backup stored on a computer on the network.
4. In the **Logical Name** box, type the name of the backup volume.
   The name you enter must use alphanumeric characters only (for example, Volume1). Do not use symbols or other special characters.

5. In the **UNC Path** box, type the path name of the volume.
   If the volume is a local volume, enter the full path name including the drive designation (for example, **`E:\BCM_Backup`**).
   If the volume is a remote volume, enter the computer IP address or computer name and the path name of the directory. For example, **`\\<IP_address>\shared_folder`** or **`\\<computer_name>\shared_folder`**.
6. In the User Name box, type the user name required to access the given path on the remote drive. The user name you enter must have full access control on the given path.
   When the domain name is required, enter **`domain_name\user_name`**.
   When the domain name is not required, enter **`user_name`**.
7. Click the **Add Volume** button.
8. Repeat steps 3 to 7 for each volume you want to add.
9. Click the **Cancel** button to close the Volume Administration screen.

Modifying volumes

1. Start BRU.
   The BRU screen appears.
2. Click the **Volume Admin** menu.
   The Volume Administration screen appears.
3. Click the **Edit** button beside the volume you want to modify.
   The volume information appears on the screen.
4. Change the volume information you want to modify.
5. Click the **Save Changes** button.
6. Click the **Cancel** button to close the Volume Administration screen.

Deleting volumes

1. Start BRU.
   The BRU screen appears.
2. Click the **Volume Admin** menu.
   The Volume Administration screen appears.
3. Click the **Delete** button beside the volume you want to delete.
   The volume information appears on the screen.
4. Click the **Delete Volume** button.
   A confirmation dialog box appears.
5. Click the **OK** button.
6. Click the **Cancel** button to close the Volume Administration screen.

Saving a backup job

When you are creating a backup job or a scheduled backup job, you can save the settings for that job. You can then load this job any time you want to run the job. This feature is particularly useful for jobs that you run several times, but do not run on a regular schedule.

1. Start BRU.
   The BRU screen appears
2. From the **Load XML File** list box, select **BCM Backup and Restore.xml**.
   The Select the Mode list box appears.
3. From the **Select the Mode** list box, select **BACKUP**.
   The BRU screen changes and displays the backup options.
4. Click the **Volume** button.
   The Volume Administration screen appears.
5. Click the **Select** button beside the volume in which you want to store the backup.
   If you want to store the backup in a volume that does not appear on the list, refer to "Adding volumes" on page 491 for information on how to add volumes.
6. If this is a scheduled job, enter the scheduled backup settings.
7. Click the **Save Job** button.
8. In the **File Name** box, type the name for this saved job.
9. Click the **Save Job** button.
   A confirmation dialog box appears.
10. Click the **Close** button.
    The backup job settings are saved.

Loading a saved backup job

When you want to run a saved backup job, you must first load that job.

1. Start BRU.
   The BRU screen appears
2. Click the **Saved Jobs** link.
   The Saved Job Files screen appears.
3. Click the **Load** link beside the job you want to load.

Deleting a saved backup job

1. Start BRU.
   The BRU screen appears
2. Click the **Saved Jobs** link.
   The Saved Job Files screen appears.

3 Click the **Delete** link beside the job you want to delete.

Transferring a file

You can transfer a text file from your computer to the directory *C:\temp* on the Business Communications Manager system.

To transfer a file to the Business Communications Manager

1 Start BRU.
The BRU screen appears

2 Click the **File Transfer** link.
The Transfer File to Server screen appears.

3 To choose a location to transfer the file to, click the **Browse** button.
The Choose File dialog box appears.

4 Navigate to the file you want to transfer to Business Communications Manager and click the **Open** button.

5 Click the **Submit** button.

6 Close the Transfer Tile to Server screen.

Resetting the BRU screen

When you reset the BRU screen, the current BRU settings are cleared and the main BRU screen appears. Saved backup jobs and scheduled backup jobs are affected when you reset the BRU screen.

To reset the BRU screen, click the **Reset** link.

Note: If a BRU process is running when you click the Reset link, a warning appears. You can choose to stop the process and continue resetting the BRU screen or you can cancel the reset and let the process continue.

Exiting from BRU

To exit from BRU, click the **Exit** link.

Chapter 22
Maintenance

This chapter contains the following information:

- "Business Communications Manager general maintenance" on page 497
- "Business Communications Manager system diagnostics and utilities" on page 498
- "Maintenance programming for telephony resources" on page 507

For information on hunt group and call-by-call usage metrics, refer to "Metrics" on page 530.

For information on physically moving telephones, refer to "Moving telephones" on page 531.

Business Communications Manager general maintenance

- "System startup" on page 497
- "Warm reset" on page 498

System startup

A system startup replaces all existing telephony programming with the default programming.

1. On the navigation tree, click the **Diagnostics** key and click the **MSC** heading.
   The **Configuration** menu is enabled.
2. From the **Configuration** menu, click **System startup**.
   The system displays a dialog box with three parameters: **Region**, **Template** and **Start DN**.
3. Select a region from the **Region** list.

   Each region has a Market Profile associated with it. For more information on Market Profiles, refer to Appendix C, "Region-based System Settings," on page 575.

Note: When you select a new region, the Template list is read-only. It is only after the system is restarted that the available templates for this region appear.

4. Type any valid value in the **start dn** box. The box displays the current value.
5. Click **OK** to apply these changes.

   The system displays a warning that the system will restart and default programming values will be restored.

Note: After the system cold start is completed, you can use a different template than the default template. From Diagnostics, MSC, System startup and select a template from the template list. However, if you select a new template, you must perform another system restart.

Warm reset

A warm reset resets the telephony portion of the system but does not affect the current telephony programming.

1. On the navigation tree, click the **Diagnostics** key and click the **MSC** heading.
   The Configuration menu option is enabled.
2. From the **Configuration** menu, click **Warm reset**.
   The system displays a warning that all active calls will be dropped.
3. Click **OK** to continue.

Business Communications Manager system diagnostics and utilities

This section provides information about Business Communications Manager diagnostic programs and utilities including:

- Business Communications Manager Performance Statistics
- Error Messages
- MIB II Information
- Alarm Banner
- Alarm Browser

Note: If you receive the error message `Telephony programming is currently not available. Please try again later.` when you click on one of the headings, this means that the part of the system that handles MSC is doing a reset. Wait about 1-1/2 minutes and try again.

Performance Statistics

Business Communications Manager provides detailed performance information for the system and the system resources. The statistics are shown in charts or table format. If a performance display is active, it is automatically updated with real-time performance information in time increments that you set.

Note: Generating statistics puts an additional workload on the Business Communications Manager server CPU, connecting network, and web client. Exercise caution when running statistics.

Generating System Performance Statistics

Business Communications Manager provides statistical information on system throughput and other performance-related information.

System performance information includes:

- System CPU Usage (graph or table format)
- Memory Usage (graph or table format).

To generate system performance statistics,

1. From the navigation tree, click the **System** heading.
   The **Performance** menu is enabled.
2. From the **Performance** menu, select the statistical information you want the system to generate, in the format of your choice.
   The chart or table appears.
3. From the **Counter Type** list, select the type of information you want the system to generate.
4. From the **Polling Interval**, select at which interval you want the system to collect the information.

Error Messages

Business Communications Manager displays error messages when system or processing errors occur. These error message appear in Unified Manager only.

Error message are made of two parts: the error string and the error number.

The error string includes the error description and the context of the error.

The error number is a three-part number that uniquely identifies the error. Be sure to note the error number when communicating with technical support center to resolve the problem.

User Actions

Some Business Communications Manager errors are caused by a wrong parameter value. For these errors, the recommended action resolves the problem. Other possible errors are caused by an internal transition of states that puts the system and the user in an error condition. In this event, assistance from technical support center is required to resolve the problem.

Note: Any Business Communications Manager errors that are not listed in this manual are advanced and require assistance from technical support center for resolution.

Errors List

In the following list, in cases where multiple errors can happen in a particular context, a wild-card representation is used.

Error Number	Description	Action
2.5.4	This is an invalid data error. There was an error in setting system date. Reason: The date, month or year component contains a zero or negative value.	Provide the correct date value.
2.xx.4	These are various errors related to an error in setting system date. Reason: The system rejected the date for various reasons. The reasons could be that it is beyond the range of dates supported. For example, 01/01/0001 is invalid date	Make sure the system date settings are valid.
2.5.6	This is an invalid data error. There was an error in setting system time. Reason: The hour or minute component contains a negative value.	Provide the correct time value.
2.xx.6	These are various errors related to an error in setting system time	Correct the error in the time format.
2.5.8	This is an invalid data error. There was an error in setting system name. Reason: The system name does not follow the standard conventions.	Make sure that your system name does not contain any special characters (hyphens are allowed, in addition to letters and digits), and that it does not exceed 15 characters in length.
5.4.59	This is an invalid configuration error. There was an error getting or setting DHCP parameters. Reason: You were adding an IP Address Range and/or Excluded Address Range and the first field you entered had a wrong key value. In the dialog boxes that appear to add the entries, the first field is a key that should match certain naming conventions. The conventions are given the label to those fields.	Follow the conventions given on the dialog boxes. For IP Address Ranges, use keys like “Rxx” and for Excluded Address Ranges, use keys like “Exx”
5.5.39	This is an invalid data value. There are invalid values for the new excluded address range. Reason: The IP Address values specified for the range are not correct. At present, each component in IP address specified in dotted format should be in the range 0-255, not including the boundary values.	Fix the value. If your IP Address range contains more than 255 addresses in it and you need to exclude a range that ends with 255 or starts with. 0, use the next upper or lower value to avoid specifying this value.
5.5.40	This is an invalid data value. There are missing values in the new excluded address range. Reason: Data for each excluded address entry should include two values - one for the start and the other for end. This error happens if one of them is missing.	Enter the missing value and click “Save”.

5.5.41	This is an invalid data value. The new excluded address range is not completely within an IP Address range. Reason: Excluded Address ranges should be completely contained within a single IP Address range specified for the scope. If a DHCP scope contains more than one IP Address range, then the excluded address ranges specified, if any, may not span outside a single IP Address range in any way. This includes overhanging outside of a single IP Address Range or spanning over multiple IP Address Range.	Fix the over-hanging problem. If required, specify multiple excluded address range. Note: As a guideline, use only one IP Address range, and specify multiple excluded ranges to exclude disjoint parts of it.
5.5.45	This is an invalid data value. The new range overlaps with an existing range Reason: This error happens if the specified excluded range overlaps with another excluded address range or with an address that is already assigned to a DHCP Client computer.	Modify the new excluded address range so that it does not overlap with another or does not include assigned IP addresses. You may also go to the client system that go the assigned address and release IP address before setting the excluded range.
5.16.68	This is an invalid operation. You can't delete the last IP Address range in the scope. Reason: The scope contains only one IP Address range and you are attempting to delete itYou must have at least one IP Address range in the scope all the time. You may modify the last entry, however.	Do not delete the last DHCP range. If you need to change it, modify it. If you do not want the DHCP scope to be operational, change its status to "Disabled". If don't want any scope operational, set the status of the DHCP Service to "Disabled".
8.4.2.	This is an invalid configuration parameter. There was an error in setting data. Reason: You tried to add a port range or filter and the key field didn't contain the characteristic prefix.	If you are adding a new port-range, make sure the "PortRange (R#)" field is like "Rxx" where "xx" is a number. If you are adding a new filter, make sure that "Filter (F#)" field looks like "Fxx" where "xx" is a number.
8.5.3	This is an invalid data value. There was an error in setting port range Reason: You are setting a port range value and the upper and lower limits are not correct or missing.	Each range should begin with a positive even number and must end with a number greater than the beginning number and must be an odd number. Further, the range values should be less than 65535 (64K)
8.8.3	There was an error in setting port range. Reason: You are setting a port range that is too big or you are starting or ending with the wrong port number. At present, only 256 ports can be set in the port-range table. Also, a port range must start with an even number and end with an odd number.	Consult the <Emphasis>Business Communications Manager IP Telephony Configuration Guide. You may not need that big a range. Reduce it to be under 256 ports in the range.
9.4.2	This is an invalid configuration parameter. There was an error in setting data. Reason: This error can happen when you are setting a community string entry, manager entry or a trap community entry. Each entry uses a characteristic key string as its field name. Use "Cxx" for community strings, "Mxx" for manager entries and "Txx" for trap community entries.	Use appropriate key strings in the dialog boxes, as suggested in their labels.
9.6.4 9.6.5 9.6.6	The object was not found. There was an error in setting <object Name> Reason: This error can happen while setting a community string entry, manager address or trap community entry. Each entry takes a characteristic key field as the first field that should follow certain conventions, and a unique number within the class. If that unique number is 0 or less, this error happens.	Specify the correct number for the key field name.

10.5.2	This is an invalid data value for requested data. Reason: This can happen happens when you enter values into a dialog box and click **Save**. If any of the fields had some strict format specified for it (dotted format for an IP address) and if you entered a wrong value, it would beep when you tab out of the field. If you ignore that beep, the GUI rejects the field and when you click **Save** it does not send the field to the Business Communications Manager system, there by causing this problem.	Follow the rules precisely. If the IP address has only 1 digit, add zeros in order to make them 3-digit in each segments of the dotted notation. For example 000.000.001. Make sure to scroll to the bottom of the screen to add all required values.
11.5.2	This is an invalid data value for password. Reason: The user was changing a user profile and the password entered in “password” and “confirm password” fields do not match.	Match the passwords.
11.19.9	Failed to Delete. Required at least one user with read-write privilege. Reason: You are attempting to delete the last existing user with READ-WRITE privilege. This operation is not permitted, as it would not allow you to make any other changes to user configuration or other system configuration.	Add another user with read-write privilege before deleting the concerned user id.
11.12.10	Failed to Update. Required at least one user with read-write privilege. Reason: You are attempting to modify the last existing user with READ-WRITE privilege. At this time, no modifications are permitted to the last READ-WRITE user.	Add another user with READ-WRITE privilege before modifying the concerned user id.
14.4.21	Invalid Configuration Parameter. Error in setting interface parameter Reason: You are setting a static route, input filter or output filter under an interface and you did not enter a correct characteristic key field in the dialog box. Values for these fields should strictly follow the convention provided in the labels for them. It should be something like “SRxx” for static routes, “IFxx” for input filters and “OFxx” for output filters.	Make sure your key names are as per convention and provide unique values for the number component.
14.17.40 14.17.41	Command failed. Error in setting action for input/output filters Reason: You were attempting to set the action for input/ output filters on the interface. The operation failed because there were no input or output filters defined for the interface.	Add an input or output filter before setting the action
14.17.68	Command failed. Error in setting static route. This problem is caused by a mismatch in destination network address or in its subnet mask specified in the route.	Match them. Bitwise AND of destination address and subnet mask should be equal to the destination address.
	The routing protocol is changed and the screen did not update.	Refresh the screen by clicking on “View Refresh” menu item.

	The routing protocol for the interface shows up as “RIP”. But no RIP configuration parameters show up on the screen	Set the routing protocol back to “NONE” and then set to “RIP” again. The RIP configuration field would show up.
14.5.77	Invalid Data Value. Static default route is not permitted in this version. Reason: You were setting a static route that was a default route for the system. In this release of Business Communications Manager, setting default routes as static routes is not permitted. The default route is managed by the “Net Link Manager” component that accepts the address of next hop router on the primary and then adds or deletes (manages) the default route in the system.	None

MIB II Information

Here is the mapping between Business Communications Manager counters shown in statistics windows and standard MIB-II variables where applicable.

This section includes:

- Counters Shown at LAN and WAN Interface Levels”
- ICMP Counters”
- UDP Counters”
- TCP Counters”
- QoS Session Counters”
- QoS Best Effort Traffic Counters”
- QoS Dropped Packets Counters”
- QoS Graph Counters”
- QoS Best Effort Queue Counters”

Counters Shown at LAN and WAN Interface Levels

1 Byte Received: ifInOctets

2 Byte Sent: ifOutOctets

3 Byte Total: no equivalent (ifInOctets and ifOutOctets)

4 Current Bandwidth: ifSpeed

5 Output Queue Length: ifOutQLen

6 Packets Outbound Discarded: ifOutDiscards

7 Packets Outbound Errors: ifOutErrors

8 Packets Received Discarded: ifInDiscards

9 Packets Received Errors: ifInErrors

10 Packets Received Non-Unicast: ifInNUcastPkts

11 Packets Received Unicast: ifInUcastPkts

12 Packets Received Unknown: ifInUnknownProtos

13 Packets Received: no equivalent

14 Packets Sent Non-Unicast: ifOutNUcastPkts

15 Packets Sent Unicast: ifOutUcastPkts

16 Packets Sent: no equivalent

17 Packets: no equivalent

ICMP Counters

Note: Shown on the Performance menu under Resources heading.

1 Messages Outbound Errors: icmpOutErrors

2 Messages Received Errors: icmpInErrors

3 Messages Received: icmpInMsgs

4 Messages Sent: icmpOutMsgs

5 Messages: no equivalent (icmpInMsgs + icmpOutMsgs)

6 Received Address Mask: icmpInAddrMasks

7 Received Address Mask Reply: icmpInAddrMaskReps

8 Received Destination Unreachable: icmpInDestUnreachs

9 Received Echo Reply: icmpInEchoReps

10 Received Echo: icmpInEchos

11 Received Parameter Problem: icmpInParmProbs

12 Received Redirect: icmpInRedirects

13 Received Source Quench: icmpInSrcQuenchs

14 Received Time Exceeded: icmpInTimeExcds

15 Received Timestamp Reply: icmpInTimestampReps

16 Received Timestamp: icmpInTimestamps

17 Sent Address Mask: icmpOutAddrMasks

18 Sent Address Mask Reply: icmpOutAddrMaskReps

19 Sent Destination Unreachable: icmpOutDestUnreachs

20 Sent Echo Reply: icmpOutEchoReps

21 Sent Echo: icmpOutEchos

22 Sent Parameter Problem: icmpOutParmProbs

23 Sent Redirect: icmpOutRedirects

24 Sent Source Quench: icmpOutSrcQuenchs

25 Sent Time Exceeded: icmpOutTimeExcds

26 Sent Timestamp Reply: icmpOutTimestampReps

27 Sent Timestamp: icmpOutTimestamps

UDP Counters

1 Datagrams No Port: udpNoPorts

2 Datagrams Received Errors: udpInErrors

3 Datagrams Received: udpInDatagrams

4 Datagrams Sent: udpOutDatagrams

5 Datagrams: no equivalent (udpInDatagrams + udpOutDataGrams)

TCP Counters

1 Connection Failures: tcpAttemptFails

2 Connections Active: tcpActiveOpens

3 Connections Established: tcpCurrEstab

4 Connections Passive: tcpPassiveOpens

5 Connections Reset: tcpEstabResets

6 Segments Received: tcpInSegs

7 Segments Retransmitted: tcpRetransSegs

8 Segments Sent: tcpOutSegs

9 Segments: no equivalent (tcpInSegs + tcpOutSegs)

QoS Session Counters

Note: These are proprietary counters implemented by QoS Provider Module.

1 Not Served Priority Sessions: The number of premium priority sessions declined by the QoS module - probably due to bandwidth restrictions.

2 Requested Priority Sessions: Total number of premium priority sessions requested

3 Served Priority Sessions: Number of premium priority sessions admitted.

QoS Best Effort Traffic Counters

Note: This is a proprietary counter.

1 Total Best-Effort Octets: Total number of octets carried in best-effort level.

2 Total Best-Effort Packets: Total number of packets carried in best-effort level.

QoS Dropped Packets Counters

Note: Proprietary counter in QoS.

1 Total Dropped Octets: Total number of octets dropped, probably due to insufficient buffer.

2 Total Dropped Packets: Total number of dropped packets.

QoS Graph Counters

1 Total Octets: Total number of octets sent by QoS.

2 Total Packets: Total number of packets sent by QoS.

3 Total Priority Octets: Total number of octets carried in premium priority.

QoS Best Effort Queue Counters

Note: This is a proprietary counter.

1 Total Queue XX Octets: Total number of octets carried at the specified queue's priority.

2 Total Queue XX Packets: Total number of packets carried at the specified queue's priority.

3 Total Queue XX Packets Dropped: Total number of packets dropped at the specified queue - probably due to insufficient buffer space.

Maintenance programming for telephony resources

When you perform maintenance on your Business Communications Manager system, you must know the system version and the status of each of your Media Bay Modules. For procedures on how to access this information, refer to the following:

- "System version" on page 507
- "Media Bay Module status" on page 508

For information on the logs generated by your Business Communications Manager system, refer to:

- "System test log" on page 511
- "System administration log" on page 512
- "Network event log" on page 513

For information on alarm codes and event messages, refer to "Alarm codes" on page 514 and "Event messages" on page 515.

If you want to run a line loopback, payload loopback, card loopback or continuity loopback test, refer to "Tests" on page 523.

For information on system statistics and metrics, refer to:

- "CSU statistics" on page 526
- "Link Status" on page 529
- "Metrics" on page 530

For information on physically moving an existing telephone, refer to "Moving telephones" on page 531.

System version

System version allows you to check the version number of the System Processor (SP) software that resides on the Media Services Card (MSC).

1. On the navigation tree, click the **Resources** key and click the **Media Services Card** heading. The version number of the software appears in the **Version** box.
2. Write the version number on the appropriate Maintenance record.

Note: You can use the version number to determine the software release and it may be required by support staff if a software fault occurs.

Media Bay Module status

Media Bay Modules selection allows you to view the status of all the modules as well as identify any device or lines connected to the system. This allows you to isolate any malfunctioning part of the system. In addition, you can use the Media Bay Module selection to disable and enable modules and devices. For more information, refer to one of the following procedures.

- "Display the Media Bay Module status" on page 508
- "Disable a module" on page 508
- "Enable a module" on page 509
- "Identify a device connected to the system" on page 509
- "Disable a device" on page 510
- "Enable a device" on page 510

Display the Media Bay Module status

Use this procedure to display module type, the number of sets connected to the module, the number of busy sets and the module's state:

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key. The window displays **Bus 02** through to **08**.
2. Click heading of the Bus you want to view. For example, **Bus 02**. The **Configuration** menu is enabled and the status information of the module associated with that bus appears.

Disable a module

You must disable a module before you replace it. In addition, you may be able to clear a hung line by disabling and enabling the affected module.

Warning: Use Page feature, on your system, prior to disabling.
Use the Page feature to inform users that you are about to disable a module. Indicate that they may experience delays in the performance of their devices.

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the heading of the Bus you want to disable. The **State** box indicates that the module is enabled. The **Configuration** menu option is enabled.
3. On the **Configuration** menu, click **Disable**. The system displays a warning that this action will disable the entire module and all of its devices.
4. Click **OK**. The system disables the module in one minute (or immediately, if the status is idle). Click **Cancel** to leave this display without disabling the module.

Enable a module

Use the following procedure to enable a disabled module.

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click heading of the Bus associated with the module you wish to enable.
   The **State** box indicates that the module is disabled and the **Configuration** menu is enabled.
3. On the **Configuration** menu, click **Enable**.
   The system displays a message indicating that the module is being enabled.

Identify a device connected to the system

You may wish to check a device's version number for compatibility with the system. Use the following procedure to display status information for any device connected to the system.

1. On the navigation tree, click the **Resources** key and click the **Media Bay Modules** key.
2. Click the key of the **Bus ##** and click the key of the **Port #**.
3. Click the **Channels** key.
4. Click the **B1** heading to display the device connected to the B1 channel or click the **B2** heading to display the device connected to the B2 channel.
   The window displays the device, its type, the version number of the device and its state.
5. If there is an add-on device attached to the telephone such as a central answering position module or a Busy Lamp Field, click the **B1** or **B2** key and click the **Addons** heading to display the add-on device.

The following table lists some of the device types that may appear on the Business Communications Manager device identification display.

Display	Explanation
T7100	T7100 telephone
T7310	T7310 telephone
M7324	M7324 telephone
1: CAP1	First CAP module attached to an M7324 telephone
2: CAP2	Second CAP module attached to an M7324 telephone
Nortel Networks ATA 2	Analog Terminal Adapter

Disable a device

Warning: Give notice that you are disabling equipment.
Inform people that you are going to disable their devices.

Warning: Pick a suitable time to disable devices. Disabling a port will disconnect users from their calls.
Do not disable devices when many people are using the Business Communications Manager system. Wait until after regular office hours.

Warning: Do not enable or disable ports during the first two minutes after plugging in your system.
If you enable or disable ports in the first two minutes after powering up, incorrect ports may be enabled or disabled. To recover from this, disable, then enable the affected modules using the **Media Bay Modules** selection.

Use the following procedure to disable a device immediately.

1. Identify the device you wish to disable. For information on how to perform this procedure, refer to "Identify a device connected to the system" on page 509.
2. Click the device you want to disable.
3. On the **Configuration** menu, click **Disable**.
   The system displays a warning that this action will disable the port.
4. Click **OK**.
   The system disables the device in one minute (or immediately, if the device is idle). Press **Cancel** to leave this display without disabling the device.

Enable a device

Use the following procedure to enable a disabled device:

1. Identify the device you wish to disable. For information on how to perform this procedure, refer to "Identify a device connected to the system" on page 509.
2. Click the device you want to enable.
3. On the **Configuration** menu, click **Enable**.
   The system displays a message indicating that the device is being enabled.

System test log

The System test log shows you a list of diagnostic test results, audits, event messages, and alarm codes. By using this feature you can check log items, any current alarms, timing of log events and the number of consecutive occurrences of an event or an alarm. In addition, you can use the **System test log** selection to erase the log.

The System test log holds a maximum of 20 items. You should check and record these items at regular intervals. Erase the log after dealing with all the items.

Use the **System test log** selection under **Diagnostics**, **MSC** to perform one of the following procedures.

- "Display information on the items in the System test log" on page 511
- "Erase the log" on page 511

Display information on the items in the System test log

You can display information on any item in the System test log using the following procedure.

1 On the navigation tree, click the **Diagnostics** key and click the **MSC** key.

2 Click the **System test log** key.
If there are no log entries, the navigation tree indicates that there are no subheadings.

3 Click an item. Information about the log item appears.
The description attribute indicates if the item is an event or alarm and includes the associated code. The severity, repeats, time and parameters of the event or alarm appears. For more information on the event or alarm, refer to "Alarm codes" on page 514 or "Event messages" on page 515.

Note: Alarms also appear in the Windows NT event log and the Alarm Database.

You must configure the Alarm Database before alarms are stored in the database. For information about how to configure the Alarm Database, refer to "Configuring the Alarm Manager" on page 482.

Any information sent to the Windows NT event log can generate an SNMP trap.

4 Write down the item on the System administration log record and repeat these steps until you record all the items.

Erase the log

You can erase log items from the System Test log using the following procedure.

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1 Choose **Diagnostics**, **MSC**, and click the **System test log** heading.

2 Click **Del All** from the menu above the navigation tree.
The system displays a message asking you to confirm that you wish to remove all of the items.

3 Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

System administration log

The System administration log keeps a record of administrative events such as sessions in which a change was made, invalid password attempts, and password changes.You can check the items in the log, check when each item in the log occurred and you can erase the log.

Note: The System administration log holds a maximum of ten items. Erase the log after dealing with all the items.

Use the **System admin log** selection under **Diagnostics, MSC** to perform one of the following procedures.

- “Display information on the items in the System Administration log” on page 512
- “Erase the log” on page 513

Display information on the items in the System Administration log

You can display information on any item in the System administration log using the following procedure.

1 Choose **Diagnostics**, **MSC**, **System admin log**.

2 Double click the **System admin log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.

3 Click an item.
Information about the log item appears. The description attribute indicates if the item is an event or alarm and includes the associated code. The severity, repeats, time and parameters of the event or alarm appears. For more information on the event or alarm, refer to “Alarm codes” on page 514 or “Event messages” on page 515.

Note: Alarms also appear in the Windows NT event log.

You must configure the Alarm Database before alarms are stored in the database. For information about how to configure the Alarm Database, refer to “Configuring the Alarm Manager” on page 482.

Any information sent to the Windows NT event log can generate an SNMP trap.

4 Write down the item on the System administration log record and repeat these steps until you record all the items.

Erase the log

You can erase log items from the System Administration log using the following procedure.

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1. Choose **Diagnostics**, **MSC**, **System admin log**.
2. Double click the **System admin log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.
3. Click **Del All** from the menu above the navigation tree.
   The system displays a message indicating that this will remove all of the items.
4. Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

Network event log

The Network event log keeps a record of events and alarms that are specific to the T1 network interface. You can check the items in the log, check when each item in the log occurred and you can erase the log.

The Network event log holds a maximum of twenty items. Erase the log after dealing with all the items.

Use the **Network event log** selection under **Diagnostics, MSC** to perform one of the following procedures.

- "Displaying information on the items in the Network event log" on page 513
- "Erase the log" on page 514

Displaying information on the items in the Network event log

You can display information on any item in the Network event log using the following procedure.

1. On the navigation tree, click the **Diagnostics** key and the **MSC** key.
2. Click the **Network event log** key to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.
3. Click an item. Information about the log item appears.
   The description attribute indicates if the item is an event or alarm and includes the associated code. The severity, repeats, time and parameters of the event or alarm appears. For more information on the event or alarm, refer to "Alarm codes" on page 514 or "Event messages" on page 515.

Note: Alarms also appear in the Windows NT event log.

Any information sent to the Windows NT event log can generate an SNMP trap.

4 Write down the item on the System administration log record and repeat these steps until you have recorded all the items.

Erase the log

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1 Choose **Diagnostics, MSC**, **Network event log**.

2 Double click the **System test log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.

3 Click **Del All** from the menu above the navigation tree.
The system displays a message indicating that this will remove all of the items.

4 Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

Alarm codes

The Business Communications Manager system generates alarm codes after system disconnections or after certain anomalies in system operation. All alarm codes appear at the Alarm telephone, in the System test log of a Maintenance session and in the Windows NT event log. For a more complete description of alarm and event codes consult your technical support representative.

Tips
You can assign the Alarm telephone in Feature settings under System programming.
Alarms have a higher severity than events. Attend to alarm codes before event messages
Alarm code information that is specific to Companion components is included in the Windows NT Event Log.

Any information sent to the Windows NT event log can generate an SNMP trap.

An alarm code may not appear until two minutes after it is triggered. If the system is powered off when the alarm is triggered, the alarm code does not appear until two minutes after the system is powered on.

Event messages

Event messages appear as items in the System administration log or the System test log of the Maintenance session. Most of these event messages can only be caused by an unusual combination of events, and should rarely occur.

Each event has a severity number. An “S” preceding this number, “S4” for example, may appear in the event message. “S9” is the most severe. If the log is full, new event messages with a higher severity number replace existing event messages of a lower severity. For this reason, you should check event messages at regular intervals. You can then deal with all messages before they are replaced. The time that the message is recorded is also provided.

Event message information that is specific to Companion components is included in the “Companion event messages (North American systems only)” on page 519.

For every event message that you see:

1. Refer to “Significant event messages” on page 515.
2. Determine if the event caused the system to automatically restart. For more information, refer to the table on “Event Message” on page 518.

Significant event messages

The following table lists event messages that are relevant to maintenance activities.

Event message		The event message is recorded when…
Evt:210-YYYZ	S4	Loopback test YYY on Trunk module Z has been started
Evt:211-YYYZ	S4	Loopback test YYY on Trunk module Z has been stopped
Evt:220-3546	S4	the Sys admin log has been cleared by the DN (3546 in this case)
Evt:221-3546	S4	the Sys test log has been cleared by the DN (3546 in this case)
Evt:222-3546	S5	the DN (3546 in this case) enters the debugging facility that is password protected
Evt:255	S9	administered mode is not supported by the module plugged into the slot
Evt:260-0302	S8	the system takes the access line on port 0302 out of service because no current was detected
Evt:261-0302	S1	the access line on port 0302 is returned to service after current was detected (see Evt:260)
Evt:268-07	S8	Dialing filter 07 has lost data due to a fault in the system memory
Evt:269-3546	S8	the Line/set filter for the DN (3546 in this case) has lost data due to a fault in the system memory
Evt:299	S1	the system powers up after a power failure
Evt:327	S5	short term alarm threshold has been surpassed in the DTM
Evt:328	S5	short term alarm threshold has been surpassed in the DTM

Event message		The event message is recorded when…
Evt:329	S5	short term alarm threshold has been surpassed in the DTM
Evt:330	S5	short term alarm threshold has been surpassed in the DTM
Evt:336	S5	long term alarm has been surpassed in the DTM
Evt:373	S5	the system restart diagnostic tool has been activated
Evt:407	S2	there are no more codes for Speed Dial numbers
Evt:408	S2	there is no more memory for Speed Dial codes
Evt:415-3546	S3	an invalid customer password has been entered by the DN (3546 in this case)
Evt:418	S7	a DN change is successful
Evt:419	S2	the time setting has been changed
Evt:421	S8	a DN change failed
Evt:422-3546	S6	a length change by the DN (3546 in this case) has been requested
Evt:423-3546	S6	an individual DN change has been requested by the DN (3546 in this case)
Evt:441	S2	a timeout occurred while waiting for ANI or DNIS digits to be received
Evt:442	S5	a timeout occurred while waiting for ANI or DNIS digits to be received
Evt:454	S5	Invalid password entered
Evt:458	S4	Call-by-Call NVRAM data is corrupt and all the values have been reset to default.
Evt:459	S9	DN length has been changed to less than 3 digits
Evt:680	S9	wireless system is disabled
Evt:681	S9	activation or recovery code entered
Evt:683	S9	new base station configuration detected
Evt:687	S4	the data driver has received a bad call reference
Evt:688	S4	the data driver has received a bad data event
Evt:689	S4	the data driver could not allocate a new index
Evt:690	S4	no response to the system within 10 seconds of being sent an initialization message
Evt:691	S4	no response to the system within 3 seconds
Evt:692	S4	a bad parameter value has been received in a stimulus message from the data device
Evt:693	S3	old data to be discarded has been detected
Evt:694	S4	RADAR flow control has received a bad stimulus message from an off-core application
Evt:695	S4	attached set denied request for a B-channel
Evt:696	S2	corrupt CLID length
Evt:697	S2	an asynchronous data report generated by SDI

Event message		The event message is recorded when…
Evt:698	S8	incorrect software key entered
Evt:799	S7	a call processing error has occurred on an ISDN line
Evt:822	S8	Alarm code 63 is sent because there are no DTMF receivers for an incoming call
Evt:882	S9	mobility data re-evaluation sequence initiated
Evt:883	S4	an invalid dial pulse signal was received by the DTM
Evt:992	S6	auto attendant error

How to read an event message

In the event message shown below, Evt799 indicates a call processing error has occurred on an ISDN line.

Evt799-031 02S7

The event number Evt799 is followed by a number representing the line or loop number, and a code for the type of error. In this example, the error has occurred on line 031 and the error code is 02.

The following table lists some of the error codes and their meanings.

Error code	Meaning
01	Internal software error. Cannot acquire the B-channel from the B-channel arbitrator.
02	Internal software error. There is no free line available for the call.
03	A call that is not on the B-channel has been attempted. These kind of calls are part of EKTS service, which is not supported by this version of the software. Check with your service provider to make sure your package does not include EKTS service.
04	Internal software error. Failed to instantiate on the chain.
05	Internal software error. Activation procedure failed.
06	Internal software error. Index conversion failed.
07	Unexpected digits on a Manual answer mode line. Configuration of the system and the network connection may not match.
09	Cannot get vterm (virtual terminal) from the Vterm Server.
0C	Internal software error. Already instantiated on the chain.

Events that cause a system restart

You should rarely see any event messages that are not described in the "Significant event messages" on page 515. If you do see one of these event messages, the system has followed its normal recovery from an unusual combination of system events. Although the problem is not a serious one, you should report repeated occurrences of the event number as soon as possible.

As a result of some events, the system automatically restarts itself. The table on the next two pages lists all the event numbers and identifies the events associated with system restarts.

Most of these events are recorded in the **System test log**. The few exceptions to this are recorded in the **System administration log**, as indicated.

Event Message	System Restart	Event Message	System Restart
101-106	Yes	400 (Admin log)	Yes
107	No	401-403	No
108-112	Yes	405-411	No
113	No	412-419 (Admin log)	No
114-116	Yes	421-423 (Admin log)	No
117	No	424-425	No
118-120	Yes	426-430	Yes
121-123	No	431	No
124-125	Yes	432	Yes
126-129	No	433	No
130	Yes	441-442	No
131-132	No	453	No
133-134	Yes	454	No
135-136	No	458-459	No
137	Yes	600-602	Yes
138-150	No	603-613	No
151	Yes	614	Yes
152	No	615-629	No
160-164	No	630	Yes
170-173	No	631-646	No
200-211	No	680	No
220 (Admin log)	No	681	No
221-222	No	683	No
223 (Admin log)	No	689-698	No

Event Message	System Restart	Event Message	System Restart
224	Yes	799	No
225-228	No	800-802	No
229 (Admin log)	No	803	Yes
230-235	No	804-807	No
245-248	Yes	808	Yes
250-256	No	809	No
260-271	Yes	810	Yes
280-283	No	811-820	No
285-298	Yes	823	Yes
299	No	824-825	No
327	No	851	No
328	No	882	No
329	No	883	No
330	No	900	No
336	No	940-943	No
373	No	950-989	No

Companion event messages (North American systems only)

Table 171 Event messages

Event message		Cause
Evt:275-3546	S8	(U.S. only) Unable to activate all registered portables. The system ran out of portable credits. One event is generated per portable that failed to activate. The repetition of the corresponding alarm code 59 indicates how many additional credits must be purchased.
Evt:301-1031	S5	The Base Station (on port 0103 in this case) cannot successfully receive the data image. Both radios belonging to the Base Station are disabled. This may occur if the flash EEPROM is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:302-1031	S5	The Base Station (on port 0103 in this case) cannot be written to during data transfer. Both radios belonging to the Base Station are disabled. The Base Station's flash EEPROM is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.

Event message		Cause
Evt:303-1031	S5	The Base Station (on port 0103 in this case) cannot be synchronized with the other Base Stations in the system. Both radios belonging to the Base Station are disabled. The Base Station hardware is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:304-1032		A B2 channel radio (radio 2 on port 0103 in this case) cannot be synchronized with other radios because of system overload.
Evt:305-01032	S5	A B2 channel radio (radio 2 on port 0103 in this case) cannot be synchronized because the B1 radio was disabled in maintenance. Both radios belonging to the Base Station (on port 0103 in this case) are disabled. The B1 radio must be operational to synchronize both radios of the Base Station with other radios in the system.Two events are raised: one for the B1 channel radio and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:306-01031	S5	A radio (0103-1 in this case) cannot be synchronized because there are no B2 channel radios. Both radios belonging to the Base Station (on port 0103 in this case) are disabled. Two events are raised: one for the B1 channel radio and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:307-0109100	S5	A recoverable RIM fault has occurred The RIM is reset. If a link is active when this error occurs, the link is dropped. The radio (0109-1 in this case) is returned to service.
Evt:307-0109101	S5	An unrecoverable RIM fault has occurred. The radio (0109-1 in this case) is disabled and taken out of service. If a link is active when this error occurs, the link is dropped. A corresponding alarm code 53 occurs.
Evt:307-0109102	S5	The built-in self-test on the Base Station has failed. The radio (0109-1 in this case) is disabled and taken out of service. If a link is active when this error occurs, the link is dropped. A corresponding alarm code 53 occurs.
Evt:308-0103	S5	The Base Station is connected to a system that supports a radio protocol that the Business Communications Manager does not understand.
Evt:664	S8	There is a bad signature.
Evt:665	S4	(U.S. only) There are insufficient radio credits.
Evt:666	S5	(U.S. only) Radio credits decreased.
Evt:667	S5	(U.S. only) UTAM keys are required.
Evt:668	S5	(U.S. only) UTAM test failed.
Evt:669	S5	Evaluation override is finished.
Evt:670	S5	Disablement test is active.
Evt:671	S5	Disablement test is finished.

Event message		Cause
Evt:672	S5	System initialization is beginning.
Evt:673	S5	System initialization is finished.
Evt:675	S5	Demo system.
Evt:831	S5	Software error dealing with Base Station.
Evt:832	S5	System problem with locating portable telephones.
Evt:833	S5	The radio driver software which directly controls the Base Stations' device has experienced an internal error.
Evt:834	S5	System problem with locating portable telephones.
Evt:835	S5	Wireless system access error.
Evt:836	S5	Wireless system access error.
Evt:837	S5	Trying to register an incompatible wireless device.
Evt:840	S5	Wireless system software error in dealing with a portable telephone.
Evt:841	S5	Wireless system software error.
Evt:842	S5	Portable does not support specific display character.
Evt:843	S5	Internal radio driver error.
Evt:848	S5	A cell manager has been unable to register with the router.
Evt:849	S5	Synchronization error.
Evt:850	S5	Synchronization error.
Evt:851	S5	Base Station software error.
Evt:852	S5	The Data Transfer server has been told by the Base Station that an error has occurred.
Evt:853	S5	The Data Transfer server has been told by the Base Station that an error has occurred.
Evt:854	S5	Invalid event for Data Transfer.
Evt:855	S5	Internal wireless subsystem software error.
Evt:856	S5	Internal wireless subsystem locator error.
Evt:859	S5	All possible wireless telephone numbers have been registered to portable telephones. No directory number is available to handle the registration Link setup request.
Evt:864	S5	A Base Station has received a corrupted stimulus message.
Evt:865	S5	The Base Station does not understand the received stimulus message. This occurs when you are trying to use a type of portable that the system does not support.
Evt:869	S5	Wireless subsystem language loading error.
Evt:870	S5	Firmware downloading to Base Station.
Evt:871	S5	Basestation download is complete.

Event message		Cause
Evt:872	S5	Wireless subsystem error.
Evt:873	S5	Wireless subsystem Common Signaling Channel server software error.
Evt:877	S5	Wireless auto-admin (Re-Eval) subsystem detected that a data re-evaluation is required.
Evt:878	S5	Wireless data re-evaluation has started.
Evt:879	S5	Wireless data re-evaluation has completed.
Evt:881	S5	Wireless auto-admin (Re-Eval) indicating that a configured cell failed to come on-line. Alarm 23 displays cell that failed.
Evt:884	S5	The Wireless auto-admin (Re-Eval) subsystem has detected an error.
Evt:885	S5	Sequencer functionality has detected an error.
Evt:886	S5	The Wireless auto-admin (Re-Eval) Initial Intelligence component has detected an error.
Evt:887	S5	The Wireless auto-admin (Re-Eval) radio Sniffing component has detected an error.
Evt:888	S5	The Wireless auto-admin (Re-Eval) Radio Manager has detected an error.

Note: Companion alarm codes appear in the Windows NT event log.

Any information sent to the Windows NT event log can generate an SNMP trap.

Tests

Business Communications Manager allows you to run tests to verify the integrity of the installation wiring for the telephone sets. Before you run any tests, use the procedure, "DN-to-port conversion" on page 525, to determine the port associated with a particular DN.

Warning: Choose an appropriate time to run tests.
A good time to run tests is after office hours.

The following messages may appear on the Alarm Telephone during Loopback tests.

Message	Explanation
EVT: 210-YYYZ	Loopback test YYY on Trunk module Z has started
EVT: 211-YYYZ	Loopback test YYY on Trunk module Z has ended

You can start and stop Loopback tests under the **Diagnostics** heading. Run only one test at a time on an DTM. You can move on to another programming task while the loopback test is running. While the loopback test is running, the green "in Service" LED on the DTM flashes.

If you administer the internal CSU on a line loopback and payload loopback, then the central office can also invoke and stop tests. In order to be able to run a payload loopback test, you must configure the DTM for extended superframe format.

The Business Communications Manager system allows you to run the following tests:

- "Line loopback test" on page 523
- "Payload loopback test" on page 524
- "Card loopback test" on page 524
- "Continuity loopback test" on page 524

Use the procedure, "Start a loopback test" on page 524, to run any of these tests.

Line loopback test

The line loopback test loops the full 1.544 Mbps signal received from the network back to the network. The looped signal regenerates without any change in the framing format and without the removal of any bipolar violations. The line loopback test can also be invoked and stopped remotely using the in-band signal or via the facility data link (FDL) in extended super frame (ESF) format.

The line loopback test must be run in coordination with the T1 or PRI service provider. Some test patterns can cause the DTM to reset. To avoid this, start the line loopback test from your system before the T1 or PRI service provider begins their test, and stop the line loopback test from your system after the T1 or PRI service provider ends their test.

Payload loopback test

The payload loopback test loops the received information bits (192 per frame) back to the network. You can also remotely invoke and stop the payload loopback test through the facility data link (FDL) in extended super frame (ESF) format.

The payload loopback test must be run in coordination with the T1 service provider. Some test patterns can cause the DTM to reset. To avoid this, start the payload loopback test from your system before the T1 service provider begins their test, and stop the payload loopback test from your system after the T1 service provider ends their test.

Card loopback test

The card edge loopback test loops the outgoing signal on the DTM back to its internal received signal path. The system disconnects signal paths to the external network.

Continuity loopback test

The continuity loopback test shorts the tip and ring pair of the receive signal path with the transmit signal path. This test allows you to check the metallic continuity of the external wiring.

Start a loopback test

Warning: Give notice that you are running a loopback test.
Calls on all T1 or PRI lines on the DTM are automatically dropped when a loopback test is invoked. Use the Page feature to notify people using the system that a test is about to begin and that calls will be disconnected.

1. Choose **Diagnostics**, **Trunk Modules**.
2. Double click the bus that contains the card you want to test. For example, **Bus 02**.
3. Double click the appropriate module on this bus. For example, **Module 1**.
4. Click **Loopback Tests**.
   The **Configuration** menu option is enabled. The loopback status box displays the type of test currently running.

Note: If there is an analog module in the media bay or the media is empty, the box displays Not equipped.

5. On the **Configuration** menu, click **Start loopback** to begin the test.
   The system displays the Loopback type selection window.
6. From the drop-down menu, select the test you want to run and then click **OK**. The options are **Line**, **Payload**, **Card edge** or **Continuity**.

Note: To end the test at any time, click Stop loopback on the Configuration menu.

DN-to-port conversion

If you know the DN of a telephone, you can determine the port associated with this DN using the following procedure.

1. Choose **Diagnostics**, **MSC**, and click the **DN-to-port conversion** heading.
2. Type the DN in the **DN to convert** box and press **Enter**.
   The system displays values in the Device port and Device channel boxes.

Debug

The Debug features are intended to be used with the assistance of your Business Communications Manager technical support team.You do not need the information provided by these features unless directed by a member of the technical support team.

Restart info

To view the Restart info:

1. Choose **Diagnostics**, **MSC**, **Debug**, and click the **Restart info** heading.
   The **Restart info** summary screen appears.
2. On the **Configuration** menu click **Clear restart info** to clear the log.

Registers

To view the Registers information:

1. Choose **Diagnostics**, **MSC**, **Debug**, **Restart info**.
2. Click the Registers heading.
   The **Registers** summary screen appears.

Message monitoring

1. Choose **Diagnostics**, **MSC**, **Debug**, and click the **Message monitoring** heading.
   The **Message monitoring** screen appears.

CSU statistics

Each DTM has an internal channel service unit (CSU). When enabled, the internal CSU monitors the quality of the received T1 signal and provides performance statistics, alarm statistics and diagnostic information.

DTMs must be individually programmed to establish parameters for collecting and measuring transmission performance statistics by the CSU.

For more information, refer to:

- "Statistics collected by the Business Communications Manager system" on page 526
- "Enable the internal CSU" on page 527
- "Check the performance statistics" on page 527
- "Check the CSU alarms" on page 528
- "Check carrier failure alarms" on page 528
- "Check bipolar violations" on page 528
- "Check short term alarms" on page 528
- "Check Defects" on page 529
- "Reset all statistics" on page 529

Statistics collected by the Business Communications Manager system

The system accumulates three performance parameters:

- errored seconds (ES)
- severely errored seconds (SES)
- unavailable seconds (UAS)

These parameters are defined as per TIA-547A. Errored seconds are enhanced to include control slip (CS) events. Only near-end performance data is recorded.

The internal CSU continuously monitors the received signal and detects four types of transmission defects:

- any active carrier failure alarms (CFA) (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI)
- the number of bipolar violations that occurred in the last minute
- any defects (loss of signal LOS, out of frame OOF, alarm indication signal AIS) that occurred in the last minute
- the number of milliseconds of short term alarms (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI) in the last minute. A short term alarm is declared when the detected defects persist for tens of milliseconds.

A carrier failure alarm (CFA) is a duration of carrier system outage. CFA types reported can be mapped to CFAs defined in TIA-547A and TR62411 as follows:

Business Communications Manager	**TIA-547A**	**TR62411**
LOS CFA	Red CFA	Red CFA
OOF CFA	Red CFA	Red CFA
AIS CFA	Red CFA	AIS CFA
RAI CFA	Yellow CFA	Yellow CFA

The criteria for declaring and clearing the alarms is selectable to meet those in TIA-547A or TR64211.

Enable the internal CSU

Use the following procedure to enable the internal CSU to gather performance statistics for your T1 lines or PRI with public interface.

1. Choose **Resources**, **Media Bay Modules**.
   The window displays **Bus 02** through to **08**.
2. Choose the appropriate bus. For example, **Bus 02**.
3. Choose **Modules on Bus**.
   The modules on this bus appear.
4. Choose the appropriate module. For example, **Module 1**.
5. Click the **T1 Parameters** heading.
6. In the **Internal CSU** box, click **On**.
   The module is temporarily disabled while the internal CSU is enabled.

Check the performance statistics

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose the appropriate bus that contains the module that you want to check.
3. Choose **Module #**, **CSU statistics**, **Performance statistics**.
4. Click the **Current interval** heading to display the duration of the current 15 minute interval of the selected card, the number of errored seconds (ES), the number of severely errored seconds (SES) and the number of unavailable time seconds (UAS).
5. Double click the **15 min intervals** heading to display statistics for 15 minute intervals in the last 24 hours, numbered from the most recent (01) to the oldest (96). Click the most recent interval. The window shows the start time of the interval.
6. Click the **24-hour summary** heading for an overall summary of the previous 24 hours.
   The **Number of intervals**, **Errored Seconds**, **Severely Errored Seconds**, **Unavailable Seconds** appear in the summary.

Check the CSU alarms

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose a bus and then choose a module.
3. Choose **CSU Statistics**, **Alarm statistics** and click the **Active alarms** heading.
   The display shows all the active alarms of the types **LOS (loss of signal)**, **OOF** (out of Frame), **RAI** (Remote alarm indicator) or **AIS** (Alarm indication signal). For more information on these types of transmission defects, refer to "Statistics collected by the Business Communications Manager system" on page 526.

Check carrier failure alarms

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose a bus and then choose a module.
3. Choose **CSU Statistics**, **Alarm statistics**, **CFA alarms**.
   The display shows **LOS (loss of signal)**, **OOF** (out of Frame), **AIS** (Alarm indication signal), **RAI** (Remote alarm indicator), Short-term alarms and Defects. For more information on these types of transmission defects, refer to "Statistics collected by the Business Communications Manager system" on page 526.
4. Choose the type of alarm you wish to view. For example, **LOS (Loss Of Signal)**.
5. Click the **Period #**.
   The display shows the Start time of the period.

Check bipolar violations

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose a bus and then choose a module.
3. Choose **CSU Statistics** and click the **Alarm statistics** heading.
   The display shows the number of bipolar violations that occurred in the last minute.

Check short term alarms

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose a bus and then choose a module.
3. Choose **CSU Statistics**, **Alarm statistics**, and click the **ShortTerm alarms** heading.
   The display shows the short term alarms and the number of milliseconds (not necessarily contiguous) that were active in the last minute.

Check Defects

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose a bus and then choose a module.
3. Choose **CSU Statistics**, **Alarm statistics**, and click the **Defects** heading.
   The display shows the first type of defect and the number of milliseconds (not necessarily contiguous) the hardware reported in the last minute.

Reset all statistics

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose a bus and then choose a module.
3. Click the **CSU Statistics** heading.
4. On the **Configuration** menu, click **Clear CSU statistics.**
   The system displays a message indicating that this will remove all of the statistics.
5. Select **OK** to erase all the current statistics and begin collecting statistics again.

Link Status

When you purchase PRI from your service provider, you can request the number of B-channels that are allocated for you to use. For example, you may want to use only 12 B-channels instead of 23 B-channels. If you do not have all of the PRI B channels, you should disable all the B-channels that you do not need.

It is recommended that the number of lines that are deprovisioned on an DTM (configured as PRI) be the same as the number of b-channels that are disabled. For example, If the DTM is on bus 7, when b-channels 13-23 are disabled, you should deprovision lines 73 to 83.

1. Choose **Diagnostics**, **Trunk Modules**.
2. Choose a bus and then choose a module.
3. Choose **B channels**.
   A list of the B channels on this module appears.
4. Click a channel, for example, **B 01**
   The display shows the status of the PRI channel.
5. On the **Configuration** menu, click **Enable** or **Disable** to change the setting for the channel.

Metrics

The following usage metrics are available with the Business Communications Manager Software:

- "CbC limit metrics" on page 530
- "Hunt Group Metrics" on page 530

CbC limit metrics

You can view statistical information on call-by-call limit settings for PRI when the protocol is set to call-by-call routing.

1 Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, **CbC limit metrics**.
The display shows the pools that supports CbC routing.

2 Choose a pool. For example, **Pool PRI-B**
The display shows the services in the pool. The services that appear depend upon the PRI protocol.

3 Select a service. For example, **Public**.
The display shows the settings for the selected service.

To clear the settings for a selected service, click **Clear metrics** on the **Configuration** menu.

Hunt Group Metrics

This feature gives you statistical information on hunt group calls.

1 Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, **Hunt Group Metrics**.
All the Hunt Groups appear.

2 Click a **Hunt Group**.
The display shows all the statistical information for the selected hunt group.

To clear the hunt group metrics, click **Clear group** on the **Configuration** menu.

PSTN fallback metrics

To view the metrics associated with VoIP calls that fallback to the PSTN network.

1 Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, and click the **PSTN fallback metrics** heading.
The Last reset time, Fallback requests and Fallback failures values appear.

To reset the metric log, on the **Configuration** menu, click **Clear data and time**.

Moving telephones

You can move a Business Communications Manager telephone to a new location within the system without losing its programmed settings. Set relocation (automatic telephone relocation) must be enabled in system programming. This makes the internal numbers, autodial settings, and personal speed dial codes remain with the telephone when it is unplugged.

Note: The set relocation feature applies to the digital telephones and ATAs only. IP telephones, such as the i2004, i2002 and i2050, always retain their programming regardless of where you move them on the LAN or WAN.

Automatic telephone relocation is disabled by default. Use the following procedure to enable set relocation.

1. Choose **Services**, **Telephony Services**, **General settings**, and click the **Feature settings** heading.
2. In the **Set relocation** box, click **Y**.

After set relocation is enabled, unplug the telephone and plug it in again at another location. It may take up to 45 seconds for the system to recognize the telephone.

Tips

All telephones being moved should be relocated before new telephones are plugged into their place. This allows the moved telephones to retain the programmed settings. If a new telephone is plugged into the system before the old telephone is reconnected at a new location, the system will give the old telephone information to the new telephone, and the old telephone will no longer be recognized by the system.

When changing a telephone internal number (in programming), wait one minute after Automatic Telephone Relocation.

When you relocate a telephone, the telephone must remain installed and connected in the new location for at least 3 minutes for the programming relocation to be complete. Moving the telephone again before the 3 minute period may result in losing the programming.

Chapter 23
Troubleshooting your Business Communications Manager system

These troubleshooting procedures allow you to solve many problems in the Business Communications Manager system. Follow these procedures before replacing any components.

Warning: Only qualified persons should service the system.
The installation and service of this unit is to be performed only by service personnel having appropriate training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.
Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to service personnel and users, the Business Communications Manager must be connected to an outlet with a third-wire ground. Service personnel must be alert to the possibility of high leakage currents becoming available on metal system surfaces during power line fault events near network lines. These leakage currents normally safely flow to Protective Earth ground via the power cord. Therefore, it is mandatory that connection to an earthed outlet is performed first and removed last when cabling to the unit. Specifically, operations requiring the unit to be powered down must have the network connections (central office lines) removed first.

For more information, refer to the following sections.

- "General troubleshooting information" on page 533
- "Problems with telephones" on page 536
- "Problems with lines" on page 537
- "Problems with optional equipment" on page 543
- "Problems with Trunk or Station Modules" on page 547
- "Problems for network or remote users" on page 548
- "Problems with Companion sets" on page 553

General troubleshooting information

- "Getting ready" on page 534
- "Types of problems" on page 534
- "Basic troubleshooting procedure" on page 534

Getting ready

Before you begin troubleshooting, gather all the information that is relevant to your network configuration such as:

- records from people who use the network
- information about other hardware and non-Business Communications Manager features within the public or private network

Warning: Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1or PRI service.

Types of problems

The problems you encounter will likely fall into one of the following categories:

Misunderstanding of a feature: A problem may be reported because a Business Communications Manager user is unfamiliar with the operation of a given feature.You may be able to solve the problem simply by demonstrating how to use the feature correctly.

Programming errors: You may encounter problems caused by errors in programming. A feature may have been programmed incorrectly or may not have been programmed at all.

Wiring connections: Wiring problems are caused by loose, unconnected, or incorrect wiring. Use the procedures in the section on checking the hardware as a guide.

Equipment defects: You may encounter problems caused by Business Communications Manager equipment defects. See the appropriate section for problems related to the system hardware.

Basic troubleshooting procedure

Use the following basic troubleshooting procedure as well as the detailed descriptions in this guide. Where more than one procedure is given for a particular problem, the procedures represent different options from which you should select just one.

1. Diagnose the trouble by determining:
   - the types of problems users have experienced
   - the frequency of the problems
   - how many telephones are affected
2. Access the system performance graphs and tables to view the system usage and any system faults. For more information, refer to “Viewing system performance and fault alarms” on page 535.

3 Check how a feature is being used. A problem may have been reported because of a misunderstanding about how a feature works. Confirm that the person who reported a problem understands the intended use and operation of any feature in question.

4 Run a Station set test [✆] [8] [0] [5].

5 Check the wiring and hardware connections.

6 If the problem persists, run a Maintenance session as described in "Maintenance programming for telephony resources" on page 507.

7 If hardware is defective, replace it. If the trouble requires expert advice, contact your Nortel Networks representative.

Viewing system performance and fault alarms

- "System performance graphs and tables" on page 535
- "Fault Alarm Banner" on page 535

System performance graphs and tables

To access the system performance graphs and tables:

1 Choose **System**.
The Performance, Fault and Tools menu options are enabled.

2 From the **Performance** menu option, select **System CPU Usage Graph**, **System CPU Usage Table**, **Memory Usage Graph** and **Memory Usage Table**.

Fault Alarm Banner

The Alarm Banner provides a window which allows you to continually monitor the Business Communications Manager system for fault alarms. The Alarm Banner is designed to stay on your desktop for quick access. The banner uses a color code to describe the severity of the alarm and provides the number of alarms for each severity level.

Note: You must enable the Alarm Service before the Alarm banner will function. For information about how to enable the Alarm Server, refer to "Alarm Service" on page 415.

To view the system fault alarm banner:

1 From the navigation tree, click **System**.
The Performance, Fault and Tools menus are enabled.

2 From the **Fault** menu, choose **Alarm Banner**.
The Alarm Banner appears.

3 To view a list of alarms of a particular severity level, click the color coded corresponding box
or
click **ALL** (white box) to browse through the complete list of system alarms, regardless of the severity level.

The Alarm Browser appears. See "Alarm Browser" on page 536 for more information.

Alarm Browser

The Alarm Browser provides detailed description of each alarm occurring within the system. The Alarm Browser contains a Repair Action box which can help you take the correct action to clear an alarm.

To view Alarm Details:

1 From the Alarm Browser screen, click the row corresponding to the alarm for which you want detailed information.
The row is highlighted.

2 From the Alarm Browser menu, click **Actions** and click **Display Details**.
The Alarm Details screen appears.

Problems with telephones

For troubleshooting information for your telephone sets, refer to one of the following items:

- "Digital telephone display is unreadable" on page 536
- "Telephone has no dial tone" on page 537

Digital telephone display is unreadable

If the trouble is with a T7310 or an M7324 telephone

1 Press [⌂] [*] [7]

2 Press **UP** or **DOWN** to adjust the display contrast to the desired level.

3 Press **OK**.

If the trouble is with a T7100 telephone

1 Press [⌂] [*] [7].

2 Press a number on the dial pad to adjust the display contrast to the desired level.

3 Press [⌂].

If the display is still unreadable, disable the telephone and replace it with a known working one and enable the working telephone. Disable the telephone using the following procedure:

1. Choose **Resources, Media Bay Modules** and then the appropriate bus.
2. From **Ports on Bus**, select the port on the bus that the telephone uses.
3. Select **Channels**.
4. Select the channel that the telephone uses.
5. From the Configuration menu, select **Disable**.

To enable the working telephone, use the preceding procedure and select **Enable** from the Configuration menu.

Telephone has no dial tone

1. Run a Station Set Test **(** 8 0 5 **)**.
2. Check for dial tone.
3. Check the display.
4. If the problem persists, replace the telephone with a known working telephone of the same type (so that the programming is retained).
5. Check the internal wiring at both the modular jack and the distribution cross-connect. A TCM port should have between 15 and 26 V DC across the Tip and Ring when the telephone is disconnected.
6. Check the line cord.

Problems with lines

The troubleshooting problems listed here focus on trouble with making calls or using lines. For more information, refer to one of the following problems:

- “Calls can be received but cannot be made” on page 538
- “Dial tone is absent on external lines” on page 538
- “Lines at a telephone are busy after call is over” on page 539
- “Auto-answer line rings at a telephone” on page 540
- “Prime telephone gets misdialed calls” on page 541
- “Selected line reads “Not in service” or “Not available”” on page 541
- “Selected line pool shows “No free lines”” on page 542

Calls can be received but cannot be made

1. If an incorrect line number or name appears (or if neither appears) on the telephone display, check the programming settings.
   OR
   If the correct line number or name appears on the telephone display, make sure the external lines are properly cross-connected.
2. Check external lines by attaching a test telephone directly on the distribution block.
3. Ensure that the 25-pair cable is properly connected from the DSM to the station set termination.
4. In the Unified Manager, verify that the DSM module is not disabled or unequipped by selecting **Resources, Media Bay Modules** and the bus that the module is on. For more information, refer to "Display the Media Bay Module status" on page 508.
5. Disable and then enable the module by selecting **Resources, Media Bay Modules** and the bus that the module is on. For more information, refer to "Disable a module" on page 508 and "Enable a module" on page 509.
6. If you still cannot make external calls, power down, then power up the system. This should be done after business hours to avoid losing calls.
7. To check the line, contact the telephone company.

Warning: Notify service provider of T1 signaling disruption.
Notify your T1 service provider before disconnecting your T1 lines, removing power to your system, or performing any other action that disrupts your T1 signaling. Failure to notify your T1 service provider may result in a loss of T1 service.

Dial tone is absent on external lines

1. Check for dial tone using a test telephone at the connections for the external line on the distribution block.
2. Make sure that a trunk module for the line is properly installed in the server or expansion cabinet.
3. Make sure that the Business Communications Manager Expansion Cabinet is properly connected to the MSC card.
4. In the Unified Manager, select **Resources, Media Bay Modules** and the bus that the module is on, to ensure that the line is not disabled. See "Display the Media Bay Module status" on page 508.

Lines at a telephone are busy after call is over

Line indicators that have been solid for a long time are the only visible indication that lines are hung. The problem may be due to one of the following:

- "A redirected line remains busy" on page 539
- "Programming is incorrect" on page 539
- "Lines require maintenance session" on page 540

A redirected line remains busy

A line that has been redirected using Line Redirection may, under some circumstances, remain busy after a call is over. If this happens, the outgoing line for the redirection also remains busy. You can clear this kind of hung line only at the telephone that was used to redirect the line.

Use the following procedure to clear the line:

1. Enter the Button Inquiry feature code ([↻] [*] [0]) at the telephone that was used to redirect the line.
2. Press the button of the redirected line.
3. Press SHOW or [#].
4. Press DROP or [*].

Both the redirected line and the outgoing line for the redirection should now be cleared.

Programming is incorrect

The supervision and/or disconnect timer programming for the line do not match the settings for the line at the central office.

Verify in the Unified Manager that your programming for the line matches the central office settings using the following procedure:

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Select the affected line.
3. Select **Trunk/Line data**.
   The line programming data appears.
4. Verify that the supervision and disconnect timer programming match the settings for the line at the central office.

Lines require maintenance session

Lines are still hung after all the above solutions have been investigated or tried out.

For lines that are hung for any other reason, you will have to run a Maintenance session and disable then re-enable the affected trunk module using the following procedure:

1. Choose **Resources, Media Bay Modules** and the bus that the module is on. Disable the module using the procedure, "Disable a module" on page 508.
2. Enable the module using the procedure, "Enable a module" on page 509.

Follow the procedures in the "Basic troubleshooting procedure" on page 534 before proceeding.

Auto-answer line rings at a telephone

The problem may be due to one of the following:

- "Installed hardware does not support disconnect supervision" on page 540
- "Line is configured as auto-answer and unsupervised" on page 540
- "Line is not equipped for disconnect supervision at the central office" on page 541
- "Trunk module's disconnect timer setting is not correct" on page 541

Installed hardware does not support disconnect supervision

You configured a loop start trunk as auto-answer but the installed hardware does not support disconnect supervision. (In this case, the symptom would be accompanied by the Alarm 62 code symptom.) If the installed hardware does not support disconnect supervision, reconfigure the trunk as manual-answer.

Line is configured as auto-answer and unsupervised

If the line is configured as auto-answer, reconfigure it as manual-answer. If the line is configured as unsupervised, reconfigure it as supervised. Use the following procedure.

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Select the affected line.
3. Select **Trunk/line** data.
4. In the **Trunk mode** field, click **Super**.

   OR

   In the **Auto answer** field, click **Manual**.

Line is not equipped for disconnect supervision at the central office

If the line is not equipped for disconnect supervision at the central office, reconfigure the trunk as manual-answer using the following procedure:

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Select the affected line.
3. Select **Trunk/line** data.
4. In the **Auto answer** field, click **Manual**.

Trunk module's disconnect timer setting is not correct

If the disconnect timer setting for the trunk module does not match the setting for the line at the central office, reconfigure it to match the setting using the following procedure:

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Select the affected line.
3. Select **Trunk/Line data**.
   The data is displayed for this line.
4. In the **Trunk mode** field, select the correct setting.

For more information, refer to "Assigning Trunk/line Data" on page 97.

Prime telephone gets misdialed calls

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. The call has been routed to the prime telephone for the incoming trunk. Perform the following steps to determine the cause:

1. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.
2. Verify all the digit strings that the switch should be sending.
3. Check that you have defined the corresponding Received number for every target line in your system.
4. Make sure that the published telephone numbers for your network are correct.

Selected line reads "Not in service" or "Not available"

The problem may be due to one of the following:

- "Line is connected to a DTM which is currently not in service" on page 542
- "Line has been disabled for maintenance purposes" on page 542
- "Line has not been provisioned" on page 542

Line is connected to a DTM which is currently not in service

Perform the following steps to determine why the DTM is not in service:

1. Check if the green LED on the DTM is flashing to indicate that service is suspended.
2. Check if any yellow LEDs are on to indicate an alarm or error condition.
3. Check if the red test LED is on to indicate that a continuity loopback test is running.
4. Check that the cable connecting the DTM to the termination point from the central office or network is properly connected.
5. Check that the DTM is properly inserted in the module bay.
6. In the Unified Manager, verify the status of the DTM. For more information, refer to the procedure, "Display the Media Bay Module status" on page 508.

Line has been disabled for maintenance purposes

If the line has been disabled, enable the line. If the line will be out of service for some time, configure another line to replace it on the telephone.

Line has not been provisioned

If the line has not been provisioned, provision it.

Selected line pool shows "No free lines"

If this happens often, there are not enough lines in the line pool to serve the number of line pool users. If this is the case, and the line pool contains loop start trunks, move the under-utilized loop start trunks from other line pools into the deficient line pool.

Problems with optional equipment

For more information on problems with optional equipment attached to the Business Communications Manager system, refer to one of the following problems

- "Problems with the ATA 2" on page 543
- "Problems with the auxiliary ringer" on page 544
- "Problems with external paging" on page 544
- "Problems with Music on Hold and Background Music" on page 544

Problems with the ATA 2

1. Check the connections to the jack.
2. Check the connections to the ATA 2.
3. Disconnect the ATA 2 and replace it with a working digital telephone. If the telephone works properly, the system and the DSM are operating properly.
4. Verify that the programming has been performed correctly.
5. If the trouble seems to be in the system or DSM, double-check all wiring and programming options.
   OR
   If the trouble seems to be with the ATA 2, disable the ATA 2 and replace it with a known working one.

For more information, refer to the *Business Communications Manager Installation and Maintenance Guide*.

Running a Maintenance session to test a ATA 2

1. Choose **Resources, Media Bay Modules** and navigate through the selections to find the ATA 2, to ensure that the ATA 2 is not disabled. See "Identify a device connected to the system" on page 509.
2. Disable the port connected to the ATA 2 using the procedure, "Disable a device" on page 510.
3. Enable the port connected to the ATA 2 using the procedure, "Enable a device" on page 510.

Problems with the auxiliary ringer

1. If the auxiliary ringer is used for Schedules (Night, Evening, or Lunch service), ensure that Schedules is activated from the control telephone.
2. Check the wiring between the auxiliary ringer generator and the ringing device.
3. Check the wiring between the auxiliary ringer generator and the distribution block.
4. Ensure that the auxiliary ringer contacts are operating properly by checking with an ohmmeter across the auxiliary ringer pin contacts.
5. Check that the auxiliary ringer pin contacts are programmed to operate in conjunction with any or all of the features in the auxiliary ringer programming chart.

   The current capacity of the Business Communications Manager relay contacts is 50 mA DC. They are designed to operate with the auxiliary ringer generator, or equivalent.

Problems with external paging

1. Use the Button Inquiry feature **(** [✆] [*] [0] **)** to verify the feature of a programmable memory button.
2. Check the wiring between the 50-pin connector and the paging amplifier.
3. Test external paging [✆] [6] [2] to ensure that it is working. The nominal output signal from the Business Communications Manager is 100 mV across 600 Ω.

Problems with Music on Hold and Background Music

Although Music on Hold and Background Music are separate features, they share the same wiring and customer-supplied music source.

1. Ensure that the proper feature access code **(** [✆] [8] [6] **)** is turned on. Adjust the volume using the volume control bar.
2. Use the Button Inquiry feature **(** [✆] [*] [0] **)** to verify the feature is on a programmable memory button.
3. If there is trouble with Music on Hold or Background Music, check the feature settings in the Unified Manager by selecting **Services, Telephony Services**, **General settings** and then **Feature settings**.
4. Check the wiring between the music source and the 50-pin connector.
5. Ensure that the music source is turned on, is operational, and the volume control is set properly.
6. Any music source with a low-output impedance (for example, less than 3,300 ohms) can be connected. The output level must be less than one volt.

Problems with module service

Check first for user problems, then wiring connections and programming errors before replacing Business Communications Manager equipment.

Warning: Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

1. Check that the module is properly inserted in the server or expansion cabinet.
2. Access **Resources** and then **Media Bay Modules**, to ensure that the module is not disabled. For more information, refer to the procedure, "Display the Media Bay Module status" on page 508.

If the problem persists
If the AC power is present and the LED indicator on the module is off, contact your customer service representative. If AC power is present and the LED indicator on the Business Communications Manager system is off, replace the Business Communications Manager system.

Note: Before you replace the Business Communications Manager system, disconnect all central office and station lines from the Business Communications Manager system. Power down the system by unplugging it.

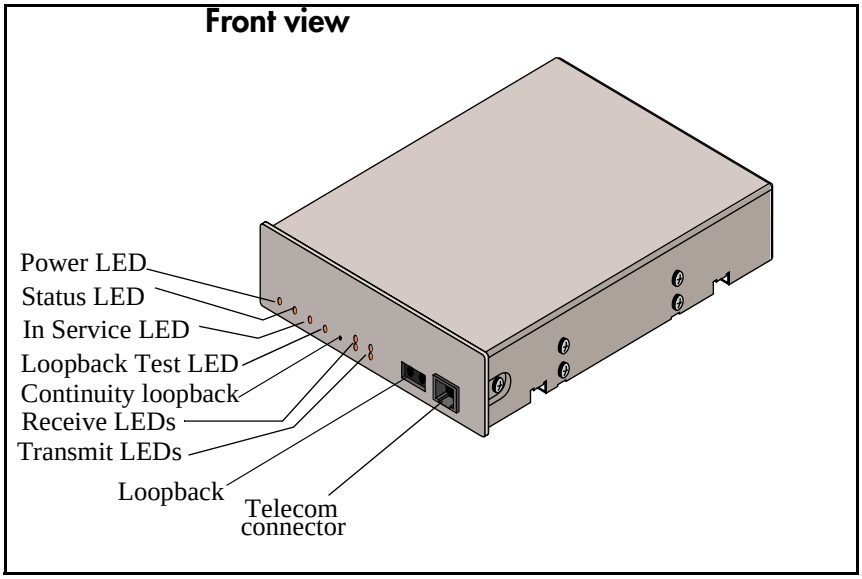
Refer to *Business Communications Manager Installation and Maintenance Guide* for information on replacing components.

Refer to the following sections for more information:

- "Digital Trunk Module trouble" on page 546
- "Monitoring the T1 or PRI signal" on page 547

Digital Trunk Module trouble

1. Choose **Resources, Media Bay Modules** and the bus that the module is on to verify that the DTM is enabled and that the lines are provisioned. For more information, refer to the procedure, "Display the Media Bay Module status" on page 508.
2. Check the LEDs on the front of the DTM.



- **Receive Alarm**: yellow LED on indicates a problem with the digital transmission being received. This half-duplex link is unusable.
- **Receive Error**: yellow LED on indicates a minor error as a result of degraded digital transmission. Possible causes are an ohmic connection, water ingress, or too long a loop.
- **Transmit Alarm**: red LED on indicates an inability to transmit. Alarm indication signal (AIS) is being transmitted to the terminating switch. This half-duplex link in unusable.
- **Transmit Error**: yellow LED on indicates a remote alarm indication (RAI) carrier failure alarm (CFA) is being sent to the terminating switch. If the Transmit Alarm is not on, this indicates a far-end or cable problem.
- **In service**: flashing green LED indicates that the T1 or PRI trunks are out of service because of a running loopback test, or because the DTM is being initialized.
- **Loopback test**: red LED on indicates a continuity loopback test is running.
- **All LEDs flashing continuously**: the DTM is being initialized.

3. In the Unified Manager, select **Resources, Telephony**, **Maintenance**, and **Tests** to run any loopback tests as appropriate.
4. Check the pinout of the cable that connects the DTM to the termination point from the T1 or PRI service provider or the external channel service unit, and check that the cable is properly connected.
5. Check with your T1 or PRI service provider to see if through-fed repeaters are used on the T1 or PRI span. The DTM does not provide the DC connection required for through-fed repeaters.

If through-fed repeaters are used on the T1 span, disable the internal CSU and connect the DTM to an external CSU.

6 If the problem persists, replace the DTM.

Caution: Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

For information on how to replace any system components, refer to the *Business Communications Manager Installation and Maintenance Guide*

Monitoring the T1 or PRI signal

If you are finding minimal faults with the T1 or PRI signal, you can monitor the signal to try and isolate the problem. The monitor jack on the DTM faceplate provides non-intrusive, bridged in-service monitoring of the T1 or PRI signal. Connect a protocol analyzer or other test equipment into the monitor jack to monitor the signal received from the network, and the signal transmitted by Business Communications Manager.

Problems with Trunk or Station Modules

1 Choose **Resources, Media Bay Modules** and the bus that the module is on to ensure that the module is not disabled. For more information, refer to the procedure, "Display the Media Bay Module status" on page 508.

2 Disable the module using the procedure, "Disable a module" on page 508.

3 Enable the module using the procedure, "Enable a module" on page 509.

For an DTM, CTM or DSM:
Check the external line by terminating a single-line telephone directly on the distribution block, or equivalent, which connects to the Trunk Module.

For the ASM:
If the ASM is still down, power down, then power up the Business Communications Manager system.

If the problem persists

1 If AC power is present and the LED indicator on the module is off, replace the module.

2 Replace the link cable.

3 Replace the module.

4 Replace the MSC.

For information on replacing components, refer to the *Business Communications Manager Installation and Maintenance Guide.*

Problems for network or remote users

Refer to one of the following items for information on how to solve network or remote user problems.

- "Remote feature code gets no response" on page 548
- "Dialed number gets ringback and the wrong person" on page 548
- "Dialed number gets dial tone instead of ringback" on page 549
- "Dialed number gets busy tone" on page 549
- "Dialed number does not get through" on page 549
- "Dialed feature code gets overflow tone" on page 550
- "Dialed feature code gets busy tone" on page 551
- "Line pool access code gets overflow tone" on page 551
- "Line pool access code gets ringback" on page 552
- "Line pool access code gets busy tone" on page 552
- "Dialed number gets no response" on page 552

Remote feature code gets no response

An Business Communications Manager user has called into another Business Communications Manager system and is trying to activate a remote feature but gets no response after dialing the feature code. Perform the following steps to determine the cause:

1. Make sure that the remote caller is dialing the feature code correctly. Use the asterisk (*) character, followed by the feature code, to activate a remote feature. (Do not use **Feature** for accessing features on a remote Business Communications Manager system.)
2. Make sure that the remote user is dialing tones, not pulses once the call is answered.

Dialed number gets ringback and the wrong person

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. The call has been routed to the prime telephone for the incoming trunk. Perform the following steps to determine why calls are being routing incorrectly:

1. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.
2. Verify all the digit strings that the switch should be sending.
3. Check that you have defined the corresponding Received number for every target line in your system.
4. Make sure that the published telephone numbers for your network are correct.
5. Make sure that the Public DN Length is long enough.

Dialed number gets dial tone instead of ringback

The remote caller has tried to reach a Business Communications Manager target line, but has reached the Business Communications Manager system instead. The system has mapped the incoming digits onto the Auto DN. Perform the following steps to determine why the remote caller cannot reach the target line:

1. Verify all the digit strings that the switch should be sending.
2. Check that you have defined the corresponding Received number for every target line in your system.
3. Check that you have defined the correct Auto DN for your system.
4. Make sure that the published telephone numbers for your network are correct.
5. Make sure that the Public DN Length is long enough.

Dialed number gets busy tone

The target line that the incoming digits map onto is busy, and there is no prime telephone for the incoming trunk. For maximum call coverage, make sure that you configure a prime telephone for every incoming trunk.

Dialed number does not get through

The problem may be due to one of the following:

- "Digits do not match Received number or Auto DN" on page 549
- "The Business Communications Manager system did not receive some or all of the incoming digits" on page 550

Digits do not match Received number or Auto DN

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. There is also no prime telephone assigned for the incoming trunk. In this case, the caller may hear overflow tone from the Business Communications Manager system or a recorded message from the originating switch. Perform the following troubleshooting steps:

1. Configure a prime telephone for every incoming trunk.
2. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.
3. Verify all the digit strings that the switch should be sending.
4. Check that you have defined a Received number for every target line in your system.
5. Make sure that the published telephone numbers for your network are correct.

The Business Communications Manager system did not receive some or all of the incoming digits

Perform the following troubleshooting steps to determine why the system is not receiving some of the incoming digits:

1. Check that the system hardware is receiving signals properly.
2. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.
3. If the switch at the far end is sending pulse signals, make sure they are being sent at the proper rate. (Pulse digits must be 300 ms or more apart for the Business Communications Manager system to receive them.)

Dialed feature code gets overflow tone

The problem may be due to one of the following:

- "Remote caller does not have access to that feature" on page 550
- "Feature code is not valid" on page 550
- "Call may originate on a telephone that uses pulse signaling" on page 550

Remote caller does not have access to that feature

Check the remote package that you assigned to the incoming trunk. Make sure that it gives the appropriate access to the remote caller.

Feature code is not valid

1. Make sure that remote callers have a correct listing of the features that are programmed for remote access.
2. Ensure that remote callers are programming the feature code correctly. Press * followed by the feature code to activate a remote feature.

Call may originate on a telephone that uses pulse signaling

The caller may be dialing on a rotary-dial telephone or on a push-button telephone that uses pulse signaling. Inform remote callers that they must dial from a push-button telephone that uses DTMF "tone" signaling.

Dialed feature code gets busy tone

A resource that the remote feature uses may currently be in use. For example, a remote caller trying to use the paging feature would get a busy tone if the auxiliary speaker were being used at the time.

If repeated attempts to use the remote feature get busy tone, there may be a malfunction in a resource that the feature uses. Check that the remote feature hardware is functioning normally.

Line pool access code gets overflow tone

The problem may be due to one of the following:

- "Remote caller does not have access to line pool" on page 551
- "Line pool access codes are invalid" on page 551
- "Call may originate on a telephone that uses pulse signaling" on page 551

Remote caller does not have access to line pool

If the published line pool access code is valid, the remote caller does not have access to that line pool. If this is the case, change the remote package for the incoming trunk so that it permits access to that line pool. Alternatively, give the remote caller a line pool access code that is permitted within the Class of Service on the incoming trunk.

Line pool access codes are invalid

If the published line pool access code is invalid, the system has attempted, without success, to match the invalid code to a Business Communications Manager target line internal number, and there is no prime telephone for the auto-answer trunk. Verify the following:

1. Published line pool access codes are correct.
2. Check that the line pool access codes have been entered correctly under **Access codes** in **System programming**.

Call may originate on a telephone that uses pulse signaling

The caller may be dialing from the network on a rotary-dial telephone or on a push-button telephone that uses pulse signaling. Inform remote callers that they must dial from a push-button telephone that uses DTMF "tone" signaling.

Line pool access code gets ringback

If the line pool access code gets ringback, the published line pool access code is invalid, and the system has routed the call to the prime telephone for the incoming trunk. Verify the following:

1. Make sure that the published line pool access codes are correct.
2. Check that the line pool codes have been entered correctly under **Services**, **Telephony Services**, **General Settings**, **Access codes**.

Line pool access code gets busy tone

The line pool access code will get a busy tone if there are not enough lines in the line pool to serve the number of users. If the line pool contains loop start trunks, enter programming and move under used loop start trunks from other line pools into the deficient line pool. Alternatively, you can create a separate line pool for remote users only.

Dialed number gets no response

This may be caused by one of the following:

- "Remote caller dials before far end is ready" on page 552
- "Line malfunction" on page 552
- "System malfunction" on page 552

Remote caller dials before far end is ready

The remote caller, after accessing a line in a line pool, may have started dialing before the far end was ready to receive digits. To avoid this problem, instruct remote callers to wait until they hear feedback before entering any digits.

Line malfunction

There may be a malfunction in the line that the remote caller accessed. If the problem is persistent, check that all lines in the affected line pool are functioning normally.

System malfunction

There may be a malfunction in the system that the caller is trying to reach. Inform the operators of the system at the far end that the dialed number is not getting through.

Problems with Companion sets

When there is a problem with a Companion set:

1. Make sure the portable is compatible with Business Communications Manager Companion Wireless software.
2. Verify that the portable is ON and that the battery is not low.
3. Establish a radio connection to get a dial tone.
4. If there is no dial tone present:
   - Verify that a dial tone is available from Business Communications Manager.
   - The portable may not be registered. If this is the case, register the portable again.
   - Check that the portable is using the correct registration slot.
   - Verify that the portable has been assigned the correct internal number by calling it from another telephone.

Rebooting the Business Communications Manager server

To reboot the Business Communications Manager server:

1. Choose **System** in the navigation tree.
   The Logoff menu is enabled.
2. On the **Logoff** menu, click **Reboot**.

   A message appears that asks you to confirm your request to reboot.
3. Click the **Yes** button to reboot.

Shutting down Business Communications Manager system

To shut down the Business Communications Manager system:

1. From the navigation tree, choose **System**.
   The Logoff menu is enabled.
2. On the **Logoff** menu, click **Shutdown**.
   A message appears that asks you to confirm your request to shut down the system.

Warning: Performing a system shutdown stops all Business Communications Manager applications and services, including IP telephony.

3. Click the **Yes** button to shut down the system.
   A Shutdown process status window is displayed and the **Done** button is enabled.
4. Click the **Done** button.
   When the shutdown is completed, your browser loses the connection with Business Communications Manager.

Appendix A
Setting Up Remote Routers for IP Telephony prioritization

This appendix includes information on setting up earlier version of BayStack routers and how to set up a range of UDP as a high priority.

Note: The information in this section is not required for recent versions of the Nortel Networks routers, such as the Passport 2430 or the Baystack ARN, that support prioritization based on the DiffServ Code Point (DSCP).

This appendix includes:

- Creating an Outbound Traffic Filter
- Sample Criteria, Ranges, and Actions for UDP Filtering

Creating an Outbound Traffic Filter

To create an outbound traffic filter:

1. In the Configuration Manager window, click **Circuits** and then click **Edit Circuits**.
   The Circuit List window appears.
2. Select a circuit.
3. Click the **Edit** button.
   The Circuit Definition screen appears with the circuit you selected highlighted.
4. On the **Protocol** menu, click **Add**.
5. Select the protocol priority from the list.
6. Click the **OK** button.
7. Click **Protocols**, **Edit Protocol Priority,** and then click **Priority/Outbound Filters**.
   The Priority/Outbound Filters window appears.
8. Click **Template**.
   The Filter Template Management window appears.
9. Enter the template name and click **Create**.
   The Create Priority/Outbound Template window appears.
10. Type a descriptive name in the Filter Name field.
11. Click **Criteria**, **Add**, **Datalink**, **IP,** and then click **Criterion**.
    The Add Range window appears. If you choose the User-Defined criterion, the Add User-Defined Field window appears first.

12 Type a minimum and maximum value to specify the range, and then click the **OK** button.
The Add Range window closes. The new criterion and ranges now appear in the Filter Information field of the Create Priority/Outbound Template window.

13 Click **Action**, **Add** and then click **action**.

14 Click the **OK** button.
The Filter Template Management window opens. The new template appears in the templates list.

15 Click **Done**.
The Priority/Outbound Filters window opens.

16 Click **Create**.
The Create Filter window opens.

17 Select a circuit in the Interfaces field.

18 Select a template in the Templates field.

19 Type a descriptive name in the Filter Name field.

20 Click **OK**.
The Priority/Outbound Filters window opens.

21 Click **Apply**.
The filter is applied to the circuit.

Sample Criteria, Ranges, and Actions for UDP Filtering

The filtering goal is to place all VoIP H.323 traffic leaving a particular interface in the high priority queue. From the BayRS Site Manager:

Use a criteria path of **Criteria**, **Add**, **IP**, **IP**, **UDP Destination Port**

The range is 28000 to 28255.

The action path is: **Action**, **IP**, **Add**, **High Queue**.

Note: This example shows how to give H.323 traffic priority over other protocols on the interface.

Appendix B
ISDN Overview

This chapter provides some general information about using ISDN lines on your Business Communications Manager system. Detailed information about ISDN is widely available through the internet. Your service provider can also provide you with specific information to help you understand what suits your requirements.

Welcome to ISDN

Integrated Services Digital Network (ISDN) technology provides a fast, accurate and reliable means of sending and receiving voice, data, images, text, and other information through the telecom network.

ISDN uses existing analog telephone wires and divides it into separate digital channels which increases bandwidth.

ISDN uses a single transport to carry multiple information types. What once required separate networks for voice, data, images, or video conferencing is now combined onto one common high-speed transport.

Nortel Networks endeavours to test all variations of ISDN PRI on Business Communications Manager; however, due to the number of variations, this is not always possible.

Analog Versus ISDN

ISDN offers significantly higher bandwidth and speed than analog transmission because of its end-to-end digital connectivity on all transmission circuits. Being digital allows ISDN lines to provide better quality signaling than analog POTS lines, and ISDN out-of band data channel signaling offers faster call set up and tear down.

While an analog line carries only a single transmission at a time, an ISDN line can carry one or more voice, data, fax, and video transmissions simultaneously.

An analog modem operating at 14.4 K takes about 4.5 minutes to transfer a 1MB data file and a 28.8K modem takes about half that time. Using one channel of an ISDN line, the transfer time is reduced to only 1 minute and if two ISDN channels are used, transfer time is just 30 seconds.

When transmitting data, the connect time for an average ISDN call is about three seconds per call, compared to about 21 seconds for the average analog modem call.

Types of ISDN Service

Two types of ISDN services (lines) are available: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). Each line is made up of separate channels known as B and D channels which transmit information simultaneously.

- BRI is known as 2B+D because it consists of two B-channels and one D-channel.
- PRI is known as 23B+D(in North America) or as 30B+D (in Europe). In North America, 23B+D consists of 23 B-channels and one D-channel (T1 carrier). In Europe, 30B+D consists of 30 B-channels and one D-channel (E1 carrier).

B Channels

B channels are the bearer channel and are used to carry voice or data information and have speeds of 64 kbps. Since each ISDN link (BRI or PRI) has more than one B-channel, a user can perform more than one transmission at the same time using a single ISDN link.

D Channels

The standard signaling protocol is transmitted over a dedicated data channel called the D-channel. The D-channel carries call setup and feature activation information to the destination and has speeds of 16 kbps (BRI) and 64 kbps PRI. Data information consists of control and signal information and for BRI only, packet-switched data such as credit card verification.

ISDN Layers

ISDN layers refer to the standards established to guide the manufacturers of ISDN equipment and are based on the OSI (Open Systems Interconnection) model. The layers include both physical connections, such as wiring, and logical connections, which are programmed in computer software.

When equipment is designed to the ISDN standard for one of the layers, it works with equipment for the layers above and below it. There are three layers at work in ISDN for Business Communications Manager. To support ISDN service, all three layers must be working properly.

- Layer 1: A physical connection that supports fundamental signaling passed between the ISDN network (your service provider) and the Business Communications Manager system. When the LED on a BRI S/T Media Bay Module configured as BRI is lit, your layer 1 is functioning.
- Layer 2: A logical connection between the central office or the far end and the Business Communications Manager system. Business Communications Manager has one or two of these connections for each BRI link, and one for each PRI link. Without Layer 2, call processing is not possible and there is no dial tone.

- Layer 3: Also a logical connection between the ISDN network (your service provider) and the Business Communications Manager system. For BRI lines, layer 3 is where call processing and service profile identifier (SPID) information is exchanged. This controls which central office services are available to the connection. For example, a network connection can be programmed to carry data calls.

Note: Throughout this chapter, references are made to Service profile identifiers (SPIDs). SPIDs are a part of the BRI National ISDN standard. SPIDs are not used in the ETSI BRI standard or on PRI.

The system of layers is important when you are installing, maintaining, and troubleshooting an ISDN system. For information about troubleshooting ISDN, see Chapter 23, Troubleshooting your Business Communications Manager system, on page 533.

ISDN Bearer Capability

Bearer capability describes the transmission standard used by the BRI or PRI line so that it can work within a larger ISDN hardware and software network.

The bearer capability for BRI and PRI is voice/speech, 3.1 kHz audio, and data (unrestricted 64 kbps, restricted 64 kbps, or 56 kbps).

Services and Features for ISDN BRI and PRI

As part of an ISDN digital network, your system supports enhanced capabilities and features, including:

- faster call set up and tear down
- high quality voice transmission
- dial-up Internet and local area network (LAN) access
- video transmission
- network name display
- name and number blocking (PRI, BRI and analog)
- access to public protocols

PRI Services and Features

These are the services and features provided over PRI lines:

- Call-by-call service selection (NI protocol)
- Emergency 911 dialing, internal extension number transmission
- access to Meridian 1 private networking (SL-1 protocol)

BRI Services and Features

These are the services and features provided over BRI lines:

- data transmission at speeds up to 128 kbps per loop (depending on the bandwidth supported by your service provider)
- shared digital lines for voice and data ISDN terminal equipment

Business Communications Manager Basic Rate Interface (BRI) also support D-channel packet service between a network and terminal connection. This allows you to add applications such as point-of-sale terminals without additional network connections.

Any analog or digital network connections can be shared by all Business Communications Manager telephones, peripherals and applications, and ISDN terminal equipment (TE).

Business Communications Manager supports the following ISDN services and features offered by ISDN service providers:

- D-channel packet service (BRI only) to support devices such as transaction terminals. Transaction terminals are used to swipe credit or debit cards and transmit the information to a financial institution in data packets.
- Calling number identification (appears on both Business Communications Manager sets and ISDN terminal equipment with the capability to show the information)
- Multi-Line hunt or DN hunting which switches a call to another ISDN line if the line usually used by the Network DN is busy. (*BRI only*)
- Subaddressing of terminal equipment (TE) on the same BRI loop. However, terminal equipment which supports sub-addressing is not commonly available in North America. (*BRI only*)

Transmission of B-channel packet data using nailed up trunks is not supported by Business Communications Manager.

Contact your ISDN service provider for more information about these services and features. For more information about ordering ISDN service in North America, see “Ordering ISDN PRI” on page 567 and “Ordering ISDN BRI” on page 567.

The terminal equipment (TE) connected to the Business Communications Manager system can use some feature codes supported by the ISDN service provider. See “ISDN services and features” in the *<Emphasis>Business Communications Manager Feature Programming Telephone Guide<Emphasis>* for more information.

Network Name Display

This feature allows ISDN to deliver the Name information of the users to those who are involved in a call that is on a public or private network. For information about programming this feature, see “Network Name Display” on page 129.

Your Business Communications Manager system displays the name of an incoming call when it is available from the service provider. If the Calling Party Name has the status of *private* it may be displayed as `Private name` if that is how the service provider has indicated that it should be displayed. If the Calling Party Name is unavailable it may be displayed as `Unknown name`.

Your system might display the name of the called party on an outgoing call, if it is provided by your service provider. Your system sends the Business Name concatenated with the set name on an outgoing call but only after the Business Name has been programmed.

The available features include:

- Receiving Connected Name
- Receiving Calling Name
- Receiving Redirected Name
- Sending Connected Name
- Sending Calling Party Name

For more information, see "Network Name Display" on page 129. Consult your customer service representative to determine which of these features is compatible with your service provider.

Name and Number Blocking (ONN)

(North America only)

When activated [✆] [8] [1] [9] allows you to block the outgoing name and/or number on a per-call basis. Name and number blocking can be used with a Business Communications Manager set. For information about programming this feature, see "ONN Blocking" on page 270.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Call by Call Service Selection for PRI (NI protocol)

PRI lines can be dynamically allocated to different service types with the Call by Call feature. PRI lines do not have to be pre-allocated to a given service type. Outgoing calls are routed through a dedicated PRI Pool and the calls can be routed based on various schedules.

The service types that may be available, depending on your service provider are described below.

- Public: Public service calls connect your Business Communications Manager set with a Central Office (CO). DID and DOD calls are supported.
- Private: Private service calls connect your Business Communications Manager set with a Virtual Private Network. DID and DOD calls are supported. A private dialing plan may be used.
- Tie: Tie services are private incoming and outgoing services that connect Private Branch Exchanges (PBX) such as Business Communications Manager.

- FX (Foreign Exchange): FX service calls logically connect your Business Communications Manager telephone to a remote CO. It provides the equivalent of local service at the distant exchange.
- Outwats: Outwats is for outgoing calls. This allows you to originate calls to telephones in a specific geographical area called a zone or band. Typically a flat monthly fee is charged for this service.
- Inwats: Inwats is a type of long distance service which allows you to receive calls originating within specified areas without a charge to the caller. A toll-free number is assigned to allow for reversed billing.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Emergency 911 Dialing

(North America only)

The ISDN PRI feature is capable of transmitting the telephone number and internal extension number of a calling station dialing 911 to the Public Switched Telephone Network (PSTN). State and local requirements for support of Emergency 911 dialing service by Customer Premises Equipment vary. Consult your local telecommunications service provider regarding compliance with applicable laws and regulations. For most installations the following configuration rules should be followed, unless local regulations require a modification.

- All PSTN connections must be over PRI.
- In order for all sets to be reached from a Public Safety Answering Position (PSAP), the system must be configured for DID access to all sets. In order to reduce confusion, the dial digits for each set should be configured to correspond to the set extension number.
- The OLI digits for each set should be identical to the DID dialed digits for the set.
- The routing table should route 911 to a PRI line pool.
- If attendant notification is required, the routing table must be set up for all 911 calls to use a dedicated line which has an appearance on the attendant console.
- The actual digit string 911 is not hard-coded into the system. More than one emergency number can be supported.

If transmission of internal extension numbers is not required or desired, then it is recommended that the person in charge of the system maintain a site map or location directory that allows emergency personnel to rapidly locate a Business Communications Manager set given its DID number. This list should be kept up to date and readily available.

Note: IP telephones

Ensure that you **do not** apply a 911 route to an IP telephone that is off the premises where the PSAP is connected to the system.

2-Way DID

With PRI the same lines can be used for receiving direct inward dialing (DID) and for making direct outward dialing (DOD) calls.

The dialing plan configured by your customer service representative determines how calls are routed. Consult your customer service representative to determine whether or not this feature is compatible with your service provider.

Dialing Plan and PRI

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing incoming and outgoing calls. All PRI calls must go through a dialing plan.

Notes about the dialing plan:

- allows incoming calls to be routed to sets based on service type and digits received
- provides the ability to map user-dialed digits to a service type on a Call by Call basis
- allows long distance carrier selection through user-dialed Carrier Access Codes

Consult your customer service representative to determine how your dialing plan is configured.

ISDN Hardware

To support connections to an ISDN network and ISDN terminal equipment, your Business Communications Manager must be equipped with a BRI S/T Media Bay Module (BRIM) or a Digital Trunk Media Bay Module (DTM) card configured for PRI.

PRI Hardware

The Digital Trunk Media Bay Module (DTM) is configured for PRI. In most PRI network configurations, you need one DTM configured as PRI to act as the primary clock reference. The only time when you may not have a DTM designated as the PRI primary clock reference is in a network where your Business Communications Manager system is connected back-to-back with another switch using a PRI link. If the other switch is loop-timed to your Business Communications Manager system, your DTM (PRI) can be designated as a timing master.

If your Business Communications Manager has more than one DTM configured as PRI, you must assign the first DTM as the primary reference, the second DTM as the secondary reference, and the third DTM as the timing master.

BRI Hardware

The loops on the BRI module can be programmed to support either network or terminal connections. This allows you to customize your arrangement of lines, voice terminals, data terminals and other ISDN equipment. This section describes some basic hardware configurations for network and terminal connections for each loop type.

A BRI module provides four loops. Each loop can be individually programmed as:

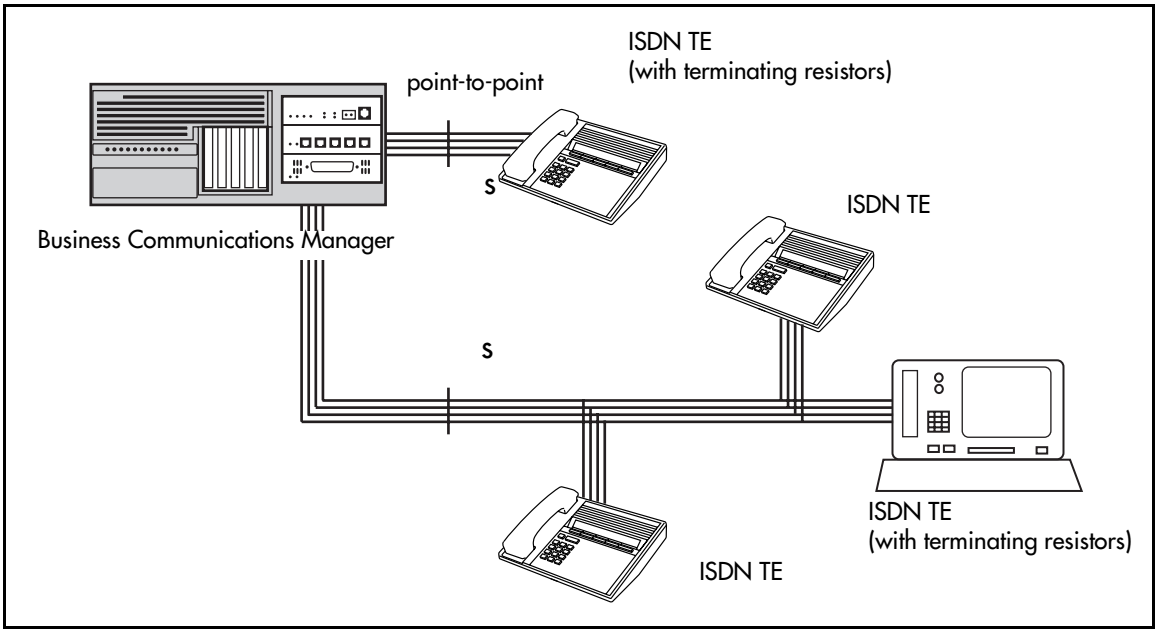
- an S reference point connection (S loop) to ISDN terminal equipment (TE), or
- a T or S reference point connection (T loop or S loop) to an ISDN network using an external NT1

S Reference Point

The S reference point connection provides either a point-to-point or point-to-multipoint digital connection between Business Communications Manager and ISDN terminal equipment (TE) that uses an S interface.

S loops support up to seven ISDN DNs, which identify TE to the Business Communications Manager system.

Figure 55 S reference point

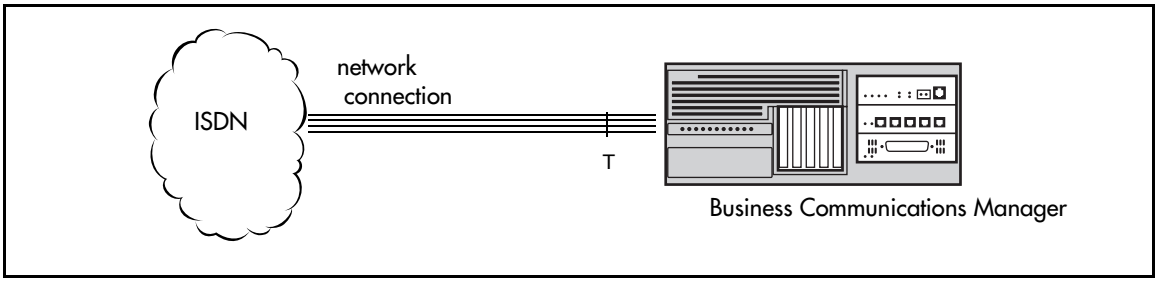


T Reference Points

The T reference point connections provide a point-to-point digital connection between the ISDN network and Business Communications Manager.

A T loop provides lines that can be shared by all Business Communications Manager telephones, peripherals and applications, and ISDN TE.

Figure 56 T reference point



A T loop can be used in combination with an S loop to provide D-packet service for a point-of-sale terminal adapter (POSTA) or other D-packet device. D-packet service is a 16 kbps data transmission service that uses the D-channel of an ISDN line.

To deliver D-packet service, a network connection (T loop) is programmed to work with a terminal connection (S loop). The loops must be on the same physical module.

Clock Source for ISDN

Systems with ISDN interfaces need to synchronize clocking with the ISDN network and any ISDN terminal equipment connected to the network. Systems synchronize clocking to the first functionally available network connection. If there are excessive errors on the reference network connection, the next available network connection is used for clock synchronization. The clock synchronization process generates alarm codes and event messages. Clock synchronization is supported by the DTM, BRI module, and FEM.

The Business Communications Manager derives timing from the network using T reference points (loops). Terminal equipment on S reference points (loops) derive timing from the Business Communications Manager system.

When you configure the network connections to the Business Communications Manager, you should take into account the system preferences for selecting loops for synchronization:

- lower numbered loops have preference over higher numbered loops
- the loop preference order is: 201, 202, 203, 204 etc.
- the system skips S and analog loops on Mod2 Card 1, when selecting a network connection for synchronization

Systems with only S loops act as timing masters for the attached terminal equipment (TE), and are not synchronized to the network. ISDN TE without access to a network connection (BRI lines) has limited or no functionality.

If your system has both a BRIM S/T configured as BRI, and a DTM configured as PRI, it is recommended that you use PRI as the primary clock source. See “PRI Hardware” on page 563.

ISDN BRI NT1 equipment

The NT1 (network termination type 1) connects an S interface (four-wire) to a U interface (two-wire). In most cases, it connects loops from a BRI module to the network connection, which uses the U interface.

The NT1 converts and reformats data so it can be transmitted to and from the S or T connection. In addition, it manages the maintenance messages travelling between the network and the NT1, and between the NT1 and the Business Communications Manager system.

The NT1 from Nortel Networks is packaged two ways:

- a stand alone package which contains one NT1 card (NTBX80XX) and a power supply (NTBX81XX)
- a modular package which contains up to 12 NT1 cards (NTBX83XX) and a power supply (NTBX86AA)

ISDN Standards Compatibility

In North America, Business Communications Manager ISDN equipment supports National ISDN standards for basic call and calling line identification services. Business Communications Manager BRI is compliant with National ISDN-1 and PRI is compliant with National ISDN-2.

Business Communications Manager does not support EKTS (Electronic Key Telephone System) or CACH (Call Appearance Call Handling).

In Europe, Business Communications Manager supports ETSI Euro and ETSI QSIG standards, and PRI SL-1 protocol.

Planning your ISDN network

Consult the *Business Communications Manager Installation and Maintenance Gui*de to determine a configuration of ISDN trunks and terminal equipment (TE) for the Business Communications Manager system, then order the appropriate ISDN capability package from your ISDN service provider.

For ISDN BRI service, your service provider supplies service profile identifiers (SPIDs), network directory numbers (Network DNs), terminal endpoint identifiers (TEIs), and other information as required to program your Business Communications Manager, TE and other ISDN equipment.

Business Communications Manager does not support any package with EKTS or CACH. EKTS is a package of features provided by the service provider and may include features such as Call Forwarding, Link, Three-Way Calling, and Calling Party Identification.

Ordering ISDN PRI

This section provides information about how to order ISDN PRI service for your Business Communications Manager.

Ordering ISDN PRI Service in Canada

In Canada, order Megalink™ service, the trade name for standard PRI service and set the Business Communications Manager equipment to the supported protocol that is identified by your service provider, either DMS-100 or NI-2.

Ordering ISDN PRI Service in United States

In the United States order PRI service from your service provider. Set the Business Communications Manager equipment to the PRI protocol indicated by your service provider.

Ordering ISDN PRI Service Outside of Canada and the United States

Outside of Canada and the United States order Euro ISDN PRI and/or BRI service from your service provider. Set the Business Communications Manager equipment to the Euro ISDN protocol.

Ordering ISDN BRI

This section provides information about how to order ISDN BRI service for your Business Communications Manager.

Ordering ISDN BRI Service in Canada

In Canada, order Microlink™ service, the trade name for standard BRI service. You can order either regular Microlink™ service, which includes the CLID feature, or Centrex Microlink™, which includes access to additional ISDN network features, including Call Forwarding).

When ordering Microlink™ service, it must be ordered with EKTS turned off. If you will be using a point-of-sale terminal adapter (POSTA), ask for D-packet service to be enabled.

Ordering ISDN BRI Service in the United States

In the U.S., regardless of the CO (Central Office) type, order National ISDN BRI-NI-1 with EKTS (Electronic Key Telephone System) turned off. Use the following packages as a guideline for ordering your National ISDN BRI-NI-1. However, we recommend using packages M or P with the Business Communications Manager system. Contact your service provider for more information about the capability packages it offers. Bellcore/National ISDN Users Forum (NIUF ISDN packages supported by Business Communications Manager (for ordering in U.S.)

	Capability	Feature set	Optional features	Point-of-sale	Voice	Data
M	Alternate voice/circuit-switched data on both B-channels	--	CLID	--	X	X
P	Alternate voice/circuit-switched data on both B-channels D-channel packet	flexible calling for voice (not supported by Business Communications Manager) Basic D-Channel Packet	additional call offering (not supported by Business Communications Manager) calling line identification	X	X	X

If you want to transmit both voice and data, and support D-channel packet service, order package P. However, Business Communications Manager does not support the flexible calling for voice and additional call offering features that are included in packageP.

Multi-Line Hunt may be ordered with your package. When a telephone number (the Network DN) in the group of numbers assigned by your service providers is busy, the Multi-Line Hunt feature connects the call to another telephone number in the group. Business Communications Manager supports the feature only on point-to-point, network connections (T loop). Check with your service provider for more information about Multi-Line Hunt.

Any of the ISDN packages will allow you to use sub-addressing, but your ISDN TE must be equipped to use sub-addressing for the feature to work.

Ordering ISDN BRI Service Outside Canada or the United States

Outside of Canada or the United States order Euro ISDN PRI and/or BRI service from your service provider. Set the Business Communications Manager equipment to the Euro ISDN protocol.

Supported ISDN Protocols

The switch used by your service provider must be running the appropriate protocol software and the correct version of that software to support ISDN PRI and BRI. Each protocol is different and supports different services. Contact your service provider to make sure that your ISDN connection has the protocol you require.

For more information on the supported protocols and services, refer to “Provisioning for Call by Call Limits with PRI” on page 188.

ISDN Programming

Most of the programming for PRI and BRI lines, and ISDN terminals is done under the **Resources/Media Bay Modules** heading in the Unified Manager. This section gives you an overview of programming for PRI and BRI lines, ISDN terminals and devices, and D-packet services.

PRI or BRI programming activity	Programming heading
View or change the Digital Trunk Media Bay Module (DTM) Configure DTM for PRI	Resources, Media Bay Modules, Bus 0#
Provision or pre-provision lines	Resources, Media Bay Modules, Bus 0#, Modules on Bus, Module 1, Provision lines
Enable or disable BRIM-S/T and DTM	Resources, Media Bay Modules, Bus 0#, Modules on Bus Module 1
View status of line, loop or port	Resources, Media Bay Modules, Bus #, Ports on Bus

Program PRI Resources

Some steps may not be necessary depending on the service you are using. For more detailed programming information, see "About the Media Bay Module Records" on page 71 and Chapter 22, Maintenance, on page 497. For complete module installation instructions and safety precautions, see the *Business Communications Manager Installation and Maintenance Guide*.

1. Collect the information supplied by your service provider to support your ISDN package.
2. Install the DTM. (For information, refer to the *Business Communications Manager Installation and Maintenance Guide.*)
3. Configure the DTM for PRI. For information on how to configure a module, see "Configuring Media Bay Modules" on page 74.
4. Configure the lines on the modules. For more information, see "Configuring Line Settings" on page 91.

Programming ISDN BRI Resources

Some steps may not be necessary depending on the service you are providing. For more detailed programming information, see "About the Media Bay Module Records" on page 71 and Chapter 22, Maintenance, on page 497. For complete module installation instructions and safety precautions, see the *Business Communications Manager Installation and Maintenance Guide*.

1. Collect the information supplied by your service provider to support your ISDN package. This includes network service profile identifiers (SPIDs) and Network DNs. If you are supporting a point-of-sale terminal adapter, you also need one or more static terminal endpoint identifiers (TEIs).
2. Install the BRIM S/T module in the Business Communications Manager system. (For information, refer to the *Business Communications Manager Installation and Maintenance*).

3 Select the module type (BRI-ST). For information on selecting a module type, see “Configuring Media Bay Modules” on page 74.

4 Select the type (T or S) for each loop. For information on how to select a loop type, see “Configuring Loops” on page 106.

5 If the module uses a T loop, enter the following configuration information (for North America only) as supplied by your service provider: the SPID assigned to the loop, the number of B-channels associated with each SPID, the Network DNs used with the network SPID, and the call type of the Network DN. Repeat the programming for the second network SPID, if any.

If the T loop is used for D-packet service: turn on the service, assign the appropriate S-loop mapping and assign the static TEIs (provided by the telco to support a point-of-sale terminal adapter or other D-packet service device) to the loop.

If the loop type is S, select the sampling used on the loop. Assign ISDN DNs to the loop and designate one of the assigned ISDN DNs to be the DN for the loop (Loop DN).

Note: You can have a maximum of 58 ISDN DNs on your system. However, there are only 28 default DNs provided. The default ISDN DN range is 597 to 694. To add to the defaults, you need to use DNs from the NA Portable Range: 565 to 597 (change DN type to **ISDN and DECT**).

Companion/DECT: If you have either a Companion wireless system, which uses the **NA Portable** range, or a DECT portable system, which uses the 597 to 694 range, ensure you do not overwrite any DNs assigned to the handsets for these systems.

6 Provision the loops and lines. For more information, see “Configuring Lines, Loops, and Routes” on page 91.

7 If you are configuring auto-answer BRI trunks to map to target lines, program the received number for the target line (see “Creating Target Lines” on page 178) to be the same as the Network DN supplied by your service provider.

From the **System DNs/All ISDN-DECT DNS/DNxx/Line Access** heading, assign the ISDN lines and target lines to the appropriate ISDN DNs. ISDN lines can also be assigned to the DNs used by Business Communications Manager telephones or any other devices connected to the Business Communications Manager system.

Program the ISDN terminals and devices with the appropriate ISDN DNs and terminal SPIDs by following the instructions that come with the devices. For more information see “Program ISDN Equipment” on page 572. If you are setting up a D-packet service, program the point-of-sale terminal adapter or other D-packet service device with the appropriate TEI from your service provider, terminal SPID, and DN by following the instructions that come with the device.

Program PRI Lines

When the hardware configuration is complete, your PRI lines are ready to be programmed. For information on programming your PRI lines, see “Provisioning for Call by Call Limits with PRI” on page 188.

Program ISDN BRI Lines

When the hardware configuration is complete, your BRI lines are ready to be programmed in the same way as analog lines. You can, for example, place them in pools and assign them to Business Communications Manager telephones and ISDN terminal equipment. However, there are some differences in the way BRI lines work that will influence how you configure them to handle incoming and outgoing calls.

For BRI lines, in most cases, your service provider supplies two SPIDs – one for each B channel. Each SPID and one or more Network DNs are associated with a single line. Calls to a Network DN come in on a specific line, and pressing a line button selects the same line every time.

If your service provider supplies you with a single SPID for both B channels, incoming and outgoing calls are handled according to the loop. The two lines provided by the BRI loop are “pooled” for both incoming and outgoing calls.

For example, if Loop 201 is programmed with a single SPID, which supports lines 061 and 062, incoming calls made to a Network DN associated with the SPID appear on either line 061 or line 062. If you press the line button for line 061, either line 061 or line 062 is selected. For loops which use a single SPID, assign both lines on a loop to a set to guarantee that all calls appear at the set.

Program Direct Inward System Access (DISA) on PRI Lines

(North America)

When a DTM is configured for PRI, all lines on that module are set to Auto Answer without Direct Inward System Access (DISA). DISA can however be accessed by one of two methods.

Method 1:

Define the DISA DN to match the trailing digits of the Called Party Number (CDN).

With Public, Private, and Tie service types, the CDN is simply truncated to the Target Line Receive Digit Length and is parsed to match the Target Line Receive Digits. DISA can be accessed by having the DISA DN match the trailing digits of the CDN. For example, with a Receive Digit Length = 4, and DISA DN = 1234, a call made to Public DN 763-1234 will be handled as follows:

- the ISDN setup message will contain a CDN of 763-1234
- the CDN will be truncated to the 4 digits, 1234
- 1234 matches the DISA DN
- the call will be answered with DISA

Method 2: (North America only)

Use incoming Call by Call (CbC) Service routing to map the call type to the DISA DN. Refer to "Configuring Call Routing" on page 117 for more information.

With FX, INWATS, 900, and SDS service types, either a Service Id (SID) or a CDN is mapped to Target Line Receive Digits. This is programmed under "Configuring Call by Call Limits" on page 186. DISA may be accessed by having the SID or CDN map to the DISA DN. This example has a Receive Digit Length = 4, DISA DN = 1234, and CbC Routing with (Service Type = FX, Map from SID = 2, Map to digits = 1234).

A call presented to the Business Communications Manager system with service type FX and SID 2 will be handled as follows:

- The ISDN setup message will specify FX with SID = 2
- The FX SID = 2 will be mapped to DISA DN digits 1234

The call will be answered with DISA.

Program ISDN Equipment

PRI modules support various applications that are enabled by PRI. For a list of the type of applications that are supported, refer to the <Emphasis>Business Communications Manager Feature Programming Telephone Guide<Emphasis>.

Terminal equipment for BRI Cards

ISDN devices and terminals connected to the Business Communications Manager system must be configured under Services, Telephony Services, Loops. You choose directory numbers for ISDN equipment from a predetermined range of DNs (597 to 694). Any of the ISDN DNs can be assigned to an S loop, but each can only be assigned to one loop and a single device. If you require more than the default 32 devices, you can use the NA Portable range of DNs (565 to 596). If you need these extra DNs, change the DN type from `NA Portable` to **`ISDN and DECT`**.

Devices on an S loop (BRI cards only)

Terminal equipment using an S loop must be assigned an ISDN directory number (ISDN DN). This allows the TE to be assigned lines and to communicate with other devices connected to the Business Communications Manager system. Each DN can be assigned to only one TE and one loop.

You assign ISDN DNs to S loops from the **Telephony Services** subheading, under **Loops**, **DNs on Loop**, **Assign DNs**. Each S loop can be programmed with eight ISDN DNs, but you cannot exceed a total of 58 ISDN DNs for the Business Communications Manager system.

S or LT Loop DN

Once you have assigned ISDN DNs to a loop, designate one of the DNs as a Loop DN. The Loop DN acts as a main ISDN DN and completes the configuration of the loop.

The ISDN terminal equipment (TE) on the loop is also programmed with its ISDN DN. See the instructions that come with the ISDN device for information about how to program it to recognize its assigned DN. Most devices will require both a terminal service profile identifier (terminal SPID) and a DN, and some will require two terminal SPIDs and two ISDN DNs. The SPID used with the device should not be confused with a SPID used for network connections using a T loop.

To create a terminal SPID for a device, add at least two zeros to the end of the ISDN DN. Add more zeros to the beginning or end of the ISDN DN until you have the length of SPID required by the TE. For example, if an ISDN telephone requires a six-digit SPID and has a DN of 667, its SPID is 066700. If the same TE requires a minimum of ten digits, the SPID is 0000066700.

Most ISDN terminals require a five-digit SPID. An ISDN PC card usually requires a ten-digit SPID. Follow the directions that come with the ISDN device to program it with a SPID and ISDN DN.

D-packet Service (BRI only)

The D-packet service supplied by the Business Communications Manager system supports a point-of-sale terminal adapter (POSTA). Connecting a POSTA allows transaction terminals (devices where you swipe credit or debit cards) to transmit information using the D channel of the BRI line, while the B channels of the BRI line remain available for voice and data calls. A special adapter links transaction equipment, such as cash registers, credit card verification rigs, and point-of-sale terminals, to the X.25 network, which is a data communications network designed to transmit information in the form of small data packets.

To support the D-packet service, your ISDN network and financial institution must be equipped with a D-packet handler. To convert the protocol used by the transaction equipment to the X.25 protocol, your ISDN network must also be equipped with an integrated X.25 PAD which works with the following versions of X.25: Datapac 32011, CCITT, T3POS, ITT and API. The ISDN service package you order must include D-packet service (for example, Package P in the United States; Microlink™ with D-channel in Canada).

Your service provider supplies a Terminal Endpoint Identifier (TEI) and DN to support D-packet service. The TEI is a number between 00 and 63 (in Canada, the default range is 21-63). Your service provider may also supply you with a DN to program your D-packet device. The DN for D-packet service becomes part of the dialing string used by the D-packet to call the packet handler.

Appendix C
Region-based System Settings

This appendix describes some of the differences in the system defaults that are used, depending on which region or template you select when you initialize your system. For information about how to initialize your system, refer to the *Business Communications Manager 2.5 Installation and Maintenance Guide*.

You select the Region at system startup. Each region is designed using a set of system defaults that provide specific functionality for the geographical area in which the system is deployed.

Core Software and Regions

Each Region setting requires a specific core software to perform correctly. Table 172 shows the core software available.

Table 172 Core software, defined by region and carrier profile

Core Software (Carrier s/w ID)	T1 CT2 Plus	T1 Etiquette	E1 Euro	E1 Global	E1 CALA
Region	Caribbean Hong Kong North American Taiwan	Caribbean Hong Kong North American Taiwan	Denmark Europe France Germany Holland Italy Norway Spain Sweden Switzerland United Kingdom	Australia CALA Global PRC	Australia CALA Global PRC
South American and Central American countries are assigned to regions in the following way: • Caribbean includes Antigua, Bahamas, Barbados, Bermuda, Cayman Islands, Dominican Republic, Jamaica, USVI, Puerto Rico, and Trinidad • CALA refers to all other Caribbean and Latin American countries with European-based standards.					

Languages

Table 173 lists the languages available for each region and a specific order in which the languages are set as default.

Table 173 Languages

Region	Language
CALA Caribbean Hong Kong North American PRC Taiwan	NA English, NA French, NA Spanish
Australia United Kingdom	UK English
Denmark	Danish, Norwegian, Swedish, NA English
France	Euro French, NA English
Germany	German, NA English
Global	NA English, NA French, NA Spanish, Turkish
Holland	Dutch, Euro French, NA English
Italy	Italian, NA English
Norway	Norwegian, Swedish, Danish, NA English
Spain	Euro Spanish, NA English
Sweden	Swedish, Norwegian, Danish, NA English
Switzerland	German, Euro French, Italian, NA English

Table 174 shows a breakdown of the language support for South American and Central American countries.

Table 174 South/Central America language breakout

Language	Spanish		English		French
Country	Dominican Republic Jamaica Puerto Rico Argentina Bolivia Chile Columbia Costa Rica Guatemala Mexico Nicaragua	Peru Panama Uruguay Venezuela El Salvador Honduras Ecuador Paraguay	St. Thomas USVI Aruba Bahamas Bermuda Curacao Trinidad Anguilla Antigua Barbados Dominica Grenada	Guyana Montserrat St. Kitts St. Lucia St. Maarten Suriname Turks & Caicos St. Vincent St. Thomas Cayman Islands Belize	Haiti

Caller ID Displays

The North American region supports the following format: 5554775 (613)

All other regions display the numbers in a continuous string of a maximum of 14 characters: 6135554775

Companding Law by Region

Table 175 shows the companding law used for each region.

Table 175 Companding law

Companding Law	
μ-law	A-law
Caribbean Hong Kong North American Taiwan	Australia CALA Denmark France Germany Global Holland Italy Norway PRC Spain Sweden Switzerland United Kingdom

ISDN Line Services

Table 176 shows the ISDN private network services that are supported by the Business Communications Manager. Table 177 shows the network-based ISDN supplementary services and the features available for each.

Table 176 ISDN line services

MCDN over PRI (SL-1)	DPNSS	DASS2	ETSI QSIG
Basic Call	Basic Call	Basic Call	Basic Call
DDI	DDI	DDI	DDI
Name display	Diversion	Originating line identity (OLI)	Name display
Number display	Redirection	Terminating Line Identity (TLI)	Number display
Centralized voice mail	Centralized voice mail	Call Charge Indication (CCI)	
Camp-on	Call Offer	Call Charge Rate Indication (CCRD)	
ISDN Call Connection Limit	Loop avoidance		
Network Call Transfer	Executive Intrusion		
Break-in	Three Party		
Trunk Route Optimization (TRO)	Route Optimization		
Trunk Anti-Tromboning			

Table 177 ISDN services, by Protocol

Protocol	Available ISDN services
NI (Caribbean. North America)	Basic Call DID Name display Number display ONN blocking
ETSI Euro (Australia. CALA, Denmark, France, Germany, Global, Holland, Hong Kong, Italy, Norway, PRC, Spain, Sweden, Switzerland, Taiwan, United Kingdom)	Basic Call DDI subaddressing (on S-loop) ETSI Call Diversion (partial rerouting) AOC-E (specific changes for Holland and Italy) MCID CLIP COLP CLIR

Mobility Services by Region

Table 178 shows the Mobility services that are supported by the Business Communications Manager, and the regions that can use each type.

Table 178 Mobility services, by region

Profile	Available Mobility Service
Caribbean North American PRC	Companion (CT2-Plus, Etiquette)
CALA	Companion (CT2-Plus)
Hong Kong Taiwan	Companion (CT2-Plus, Etiquette) DECT
Australia Denmark France Germany Global Holland Italy Norway Spain Sweden Switzerland United Kingdom	DECT

Media Bay Module Availability by Region

Some of the media bay modules are customized for a specific type of line and are not available to all regions. Table 179 lists a cross-reference between regions and the type of modules that can be used within the related area.

Table 179 Module availability, by profile

Region	DSM16/DSM32	ASM	CTM/CTM8	4X16	BRI	DTM	DECT
Australia	✓	✓			✓	✓	✓
Caribbean	✓	✓	✓	✓	✓	✓	
CALA	✓	✓	✓	✓	✓	✓	
Denmark	✓	✓			✓	✓	✓
France	✓	✓			✓	✓	✓
Germany	✓	✓			✓	✓	✓
Global	✓	✓	✓	✓	✓	✓	✓
Holland	✓	✓			✓	✓	✓
Hong Kong	✓	✓	✓	✓	✓	✓	✓
Italy	✓	✓			✓	✓	✓
North American	✓	✓	✓	✓	✓	✓	
Norway	✓	✓			✓	✓	✓
PRC	✓	✓	✓	✓	✓	✓	
Spain	✓	✓			✓	✓	✓
Sweden	✓	✓			✓	✓	✓
Switzerland	✓	✓			✓	✓	✓
Taiwan	✓	✓	✓	✓	✓	✓	✓
United Kingdom	✓	✓			✓	✓	✓

Trunk Availability by Region

Trunk Modules may be connected to the Business Communications Manager system using the Fiber Expansion Module (FEM). Table 179 provides a cross-reference between regions and the Trunk Modules you can connect to the FEM.

Table 180 Trunk availability, by region

Region	BRI S/T 2/4	BRI U2/4	PRI ETSI = 30 channels NA = 23 channels	Analog DID	E&M	CLASS	Country-specific analog trunk card
Australia	✓		✓				✓
CALA	✓	✓	✓	✓	✓	✓	
Caribbean	✓	✓	✓	✓	✓	✓	
Denmark	✓		✓				
France	✓		✓				✓
Germany	✓		✓				✓
Global	✓		✓		✓	✓	
Holland	✓		✓				✓
Hong Kong	✓		✓	✓	✓	✓	
Italy	✓		✓				
North American	✓	✓	✓	✓	✓	✓	
Norway	✓		✓				
PRC	✓		✓		✓	✓	
Spain	✓		✓				
Sweden	✓		✓				
Switzerland	✓		✓				
Taiwan	✓		✓	✓	✓	✓	
United Kingdom	✓		✓				✓

Table 181 PRI line protocol supported, by region

Region	BRI T side	BRI S side	PRI	T1
Australia	ISDN ETSI 300 403	ISDN ETSI 300 102	DASS2 DPNSS MCDN ISDN ETSI 300 403, ETSI QSIG 300 239,	
Brazil CALA	ISDN ETSI 300 403, ETSI QSIG 300 239	ISDN ETSI 300 102	ETSI QSIG 300 239, ISDN ETSI 300 403, MCDN	
Caribbean North American	NI-2	NI-2	NI-2 4ESS DMS100 DMS250 MCDN	Loop E&M DID Ground Fixed trunk types
Hong Kong Taiwan	ITU-T	ITU-T	ITU-T	Loop E&M DID Ground Fixed trunk types
Denmark France Germany Global Holland Norway PRC Spain Sweden Switzerland	ETSI QSIG 300 239, ISDN ETSI 300 403	ISDN ETSI 300 102	DASS2 DPNSS MCDN ETSI QSIG 300 239 ISDN ETSI 300 403	
Italy	ISDN ETSI 300 102 ETSI QSIG 300 239	ISDN ETSI 300 102	DASS2 DPNSS MCDN ETSI QSIG 300 239 ISDN ETSI 300 102	
United Kingdom	ETSI QSIG 300 239, ISDN ETSI 300 403	ISDN ETSI 300 102	DASS2 DPNSS MCDN ETSI QSIG 300 239 ISDN ETSI 300 403	

BRI and PRI line types

Table 182 provides a description of the types of lines that BRI and PRI trunks can provide. These are set under Resources/Media Bay Modules/Bus XX/Module X on the Unified Manager.

Note that some of these line types are only available when specific regions are chosen.

Table 182 BRI and PRI line types (DTM and BRI modules)

Digital trunk types	Description
T1	digital line that carries data on 24 channels at 1.544 Mbps (North American); 30 channels at 2,048 Mbps (Europe) Loop, E&M, DID and ground start lines are also versions of T1 lines. You can program auto-answer T1 loop start, T1 E&M trunks, T1 DID, T1 ground start trunks, PRI and IP trunks to map to target lines to provide for attendant bypass (calling directly to a department or individual) and line concentration (one trunk can map onto several target lines).
DID	This is a type of T1 trunk line that allows an outside caller to dial directly into a line on the Business Communications Manager.
Loop	This is a type of T1 line. This type of line is used on systems where the service provider supports disconnect supervision for the digital loop start trunks. These trunks provide remote access to the Business Communications Manager from the public network. This trunk must have disconnect supervision to allow the trunk to be set to auto-answer, which provides the remote access portal.
Ground	T1-groundstart trunk These lines offer the same features as loop start trunks, but are used when the local service provider does not support disconnect supervision for digital loop start trunks. Ground start trunks work with T1 only. By configuring lines as ground start, the system will be able to recognize when a call is released at the far end.
E&M	T1 and E&M. This type of trunk line is used to create simple network connections to other phone systems. This trunk always operates in a disconnected supervised mode.
PRI	ISDN interface with 23 B channels and 1 D channel at 1.544 MBps (in Europe: 30 B channels and 2 D channels at 2.048 Mbps) This is the module that controls system timing. These lines give you incoming and outgoing access to an ISDN network and are auto-answer trunks, by default. These lines provide a fast, accurate and reliable means of sending and receiving data, images, text and voice information. using PRI lines allows for faster transmission speeds and the addition of a variety of powerful business applications, including remote LAN access, video conferencing, file transfer and internet access.
BRI	ISDN loop that provides both T, S and U2 and U4 (region-specific) reference point loops. These loops can support both network (T and S loops) and terminal equipment (S loop) connections. This type of line provides incoming and outgoing access to an ISDN network. ETSI ISDN BRI is the European Telecommunications Standards Institute specification for BRI ISDN service. BRI provides two bearer B-channels operating at 64 kbits/s and a data D-channel which operates at 16 kbits/s. The D-channel is used primarily to carry call information. Like loop start trunks, BRI lines can be configured as manual-answer or auto-answer.
DASS2	(British) Trunk provides multi-line IDA interconnection to the British Telecom network.

Table 182 BRI and PRI line types (DTM and BRI modules) (Continued)

Digital trunk types	Description
DPNSS	(international term: Q.Sig or Q.931) a digital private network signaling system which allows phone systems from different manufacturers to be tied together over E1 lines, offering significant enhancements to Business Communications Manager networking capabilities. DPNSS makes it easier to support centralized network functionality within private networks, for operators and attendants dealing with large numbers of calls. Its routing capabilities provide more of the larger-network capabilities without the expense of installing a new system, re-configuring all the nodes and worrying about a lot of downtime. Most functionality over DPNSS lines is transparent once the DPNSS is programmed into the system. DPNSS allows a local node, acting as a terminating node, to communicate with other PBXs over the network using E1 lines. For example, corporate offices separated geographically can be linked over DPNSS lines to other Business Communications Manager systems, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Business Communications Manager systems to function like a private network.
Analog trunk types	
Public	Provides potential access for any set on the system.
Private	Provides potential access for a specific set.

Defining Time Zones by Country and Language

Time zones are based on the actual time zone where the Business Communications Manager base unit is located. The Time Zone dropdown list on the initialization screen, allows you to be very specific in choosing a compatible time zone. If your exact location is not on the list, choose the one with the time zone closest to you. Note that some time zones are individualized because they do not switch from Standard Time to Daylight Saving Time. For example, this is the case for Saskatchewan.

The format of the time and date changes are based on the prime language of the region.Table 183 provides a list of formats based on language or country.

Table 183 Time/date formats based on language

Language/Country	Time/Date format
Danish	2001-01-01 13:57
Dutch	1 Jan 01 13:57
EuroFrench	1 jan 13:57
EuroSpanish	1 Ene 13:57
German	1 Jan 13:57
Italian	1 Gen 13:57
NA English	Jan 1 1:57 pm
NA French	2001-01-01 13:57
NA Spanish	Ene 1 1:57 pm
Norwegian	1 Jan 13:57
Swedish	2001-01-01 13:57
Turkish	1 Ock 13:57
UK English	1 Jan 1:57 pm

System Defaults

Table 184 compares the system defaults for the North American, Global and UK regions. In addition, the following functionality applies:

- Regions for Denmark, Holland and Sweden are the same as the Global region except for the default to local languages and local tones and cadences.
- The Region for the Caribbean is the same as the North American region except that it supports the M7000 telephone.
- The Region for CALA is the same as the Caribbean region, except NI ISDN is replaced by ETSI ISDN (u-law).
- The Region for Europe is the same as the United Kingdom region except there are no default dialing restrictions, and ATA parameters are set to European values.

Table 184 Region defaults

Functionality	Attribute	North American	Global	United Kingdom
Direct Dial Access code		0	0	0
DTMF parameters	Tone duration	120 msec	120 msec	120 msec
	Pause time	1.5	1.5	3.5
	Interdigit time	80 msec	80 msec	100 msec
Conference tone		disabled	disabled	enabled
Call Back Kill time		180 sec	180 sec	360 sec
PCM Companding Law		mu-law	a-law EBI	a-law EBI
Race Integration		disabled	disabled	disabled
OLI digits		fixed 10 digits	fixed 10 digits	variable length a maximum of 8
Dial Tone Detection		enabled	enabled	enabled
Hunt Groups	Show in second	disabled	disabled	disabled
	Default delay	4 ring cycles	4 ring cycles	4 ring cycles
	Queue timeout	60 sec	60 sec	60 sec
	If busy	busy tone	busy tone	busy tone
	Mode	broadcast	broadcast	sequential
Target line if busy setting		prime	prime	busy tone
M7000 set		disabled	enabled	enabled
Fax switch		enabled	enabled	enabled
Service Schedule time	Night	start 23:00 end 07:00	start 23:00 end 07:00	start 23:00 end 07:00
	Evening	start 17:00 end 23:00	start 17:00 end 23:00	start 17:00 end 23:00
	Lunch	start 12:00 end 13:00	start 12:00 end 13:00	start 12:00 end 13:00
	Service 4	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00

Table 184 Region defaults

Functionality	Attribute	North American	Global	United Kingdom
	Service 5	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00
	Service 6	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00
Call Forward Delay	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	2 ring cycles
	Options	• 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles
DRT Delay	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	4 ring cycles
	Options	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles • 10 ring cycles	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • 6 ring cycles
Handsfree		none	none	none
Pickup Group		none	none	none
Remind Delay		60 secs	60 secs	60 secs
Allow SLR		disabled	disabled	disabled
Transfer Callback	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	4 ring cycles
	Options	• 3 ring cycles • 4 ring cycles • 5 ring cycles • 6 ring cycles • 12 ring cycles	• 3 ring cycles • 4 ring cycles • 5 ring cycles • 6 ring cycles • 12 ring cycles	• 3 ring cycles • 4 ring cycles • 5 ring cycles • 6 ring cycles • 12 ring cycles
Dialling Plan		market dependent (defined in application but controlled by market profile ID)	market dependent (defined in application but controlled by market profile ID)	market dependent (defined in application but controlled by market profile ID)
ONN Blocking	VSC for analog tone	n/a	n/a	141
	VSC for analog pulse	n/a	n/a	141
	VSC for BRI	n/a	n/a	141
	VSC for PRI	n/a	n/a	141
	State for BRI/PRI	n/a	n/a	send feature code

Table 184 Region defaults

Functionality	Attribute	North American	Global	United Kingdom
Default CO lines		2	2	4
UTAM		enabled	disabled	disabled
	Portable credits	0	defined in the application (max)	n/a
Release reason	Release text	none	none	detail
	Release code	disabled	disabled	disabled
	Display duration	3 sec	3 sec	3 sec
Overlap Receiving		disabled	enabled	disabled
Local Number length for ISDN overlap receiving		8	8	8
Tandem alerting		disabled	disabled	disabled
TON/NPI		national/E.164	national/E.164	unknown/unknown
National number length		10	10	0
national number prepend		n/a	n/a	0
Provide tone on PRI		enabled	n/a	disabled

Voice Mail Regions

The Voice Mail portion of the Business Communications Manager application also has a region setting that defines some call-management-related system defaults.

The Voice Mail region is specified at system initialization and start up when you run the Quick Start Wizard.

Table 185 lists the default prime language for the countries (regions) where the voice mail application is supported.

Table 185 Voice Mail default voice mail languages by country

Country	Default voice mail language
North America	NA English
UK	UK English
Australia	NA English
Denmark	Danish
Holland	Dutch
Sweden	Swedish
France	Euro French
CALA	LA Spanish
Caribbean	NA English
Europe	UK English
Germany	German
Global	NA English
Italy	Italian
Norway	Norwegian
Spain	Spanish
Switzerland	German
Hong Kong	NA English
PRC	Mandarin (Taiwan)
Taiwan	Mandarin (Taiwan)

Table 186 lists the feature default settings, based on region.

Table 186 Feature defaults, by region/country

Feature	Countries that use this default
Compose message start key #	All countries
Start AMIS key (#)	All countries
Primary and Secondary language toggle key (9)	All countries (not used in Brazil and CALA)
Operator Revert key (0)	All countries.

Table 186 Feature defaults, by region/country (Continued)

Feature	Countries that use this default
Mailbox login keys (*)	North America CALA Caribbean Hong Kong PRC Taiwan
Mailbox login keys (8)	UK Australia Denmark Holland Sweden France Europe Germany Global Italy Norway Spain Switzerland
AMIS (enabled)	All countries
Bilingualism enabled	All countries
digital network access (enabled)	All countries
Fax feature available (enabled)	All countries
Application name string (VM)	All countries
Touch Tone Gateway (enabled)	UK
Touch Tone Gateway (disabled)	All countries except the UK
Group list lead digit (9)	All countries
Max local number length (7)	North America Holland France Caribbean Europe Germany Global Italy Norway Spain Switzerland

Table 186 Feature defaults, by region/country (Continued)

Feature	Countries that use this default
Max local number length (7)	North America Holland France Caribbean Europe Germany Global Italy Norway Spain Switzerland
Max local number length (8)	Australia Denmark Sweden Brazil CALA
Max. local number length (11)	UK Hong Kong PRC Taiwan

Appendix D
Button programming: Features

This chapter describes the Button Programming Feature settings that you can assign to a set. (**Services/Telephony Services/System DNs/Available DNs/DNxx/User Preferences/Button Programming/Button ##**).

Note that some of these features need other system settings in order to work.

- Some of the buttons are controlled by features located under **Services/Telephony Services/ System DNs/Available DNs/DNxx/Capabilities**). Paging is an example of a feature that requires other settings.
- Some features also require that the service be available on the line from your telephone service provider. The types of lines provided are also determined by what region is chosen for your system. MCID (malicious call identification) is an example of this type of feature.

Table 187 Button Programming Feature settings

Set command	Feature	Description
	None	Button is configured for button programming, but nothing has been entered.
0	Speed dial	This button activates the speed dial feature. The telephone prompts the user for a speed dial code.
1	Send Message	Send a message to another set within the network
#1	Cancel Send Message	Cancel a message you sent to another set within the network
2	Ring again	Sets Ring again feature.
3	Conference/Transfer	Initiates call between three parties.
4	Call Forward	Allows the user to enter a number to call forward current telephone.
5	Last number redial	Causes set to redial the last number it received.
7	Contrast	Allows the user to adjust contrast on the display.
60	Page - General	Allows the user to page all sets.
61	Page - Zone	Allows the user to page a specific zone which is identified within the Button programming.
62	Page - Speaker	Allows the user to page through the speaker on a specific telephone.
63	Page - Speaker and zone	Allows the user to page through the speaker on telephones in a specific zone, which is identified within Button programming.
64	Line Pool	Allows the user to access a line pool. Either specific pools assigned to the telephone, or other general pools. The pool this button accesses is specified during Button Programming for this feature.
65	Reply message	Allows the user to access messages and send a reply to the message sender.
#65	Cancel Message Waiting	Allows the user to cancel the message waiting indicator.
66	Voice call	Allows the user to make an announcement or begin a call through the speaker of another telephone.

Table 187 Button Programming Feature settings

Set command	Feature	Description
67	Saved Number Redial	Allows the user to redial a number that they saved while on the call.
68	Restriction override	Allows the user to override any restrictions for the call they are trying to dial.
69	Priority Call	Allows the user to access a telephone that is currently busy.
70	Transfer	Allows the user to transfer an existing call to another telephone.
#70	Transfer - Cancel	Transfer a 70 action.
71	Link	Activates the Link command, which allows the user to access special features on a remote PBX.
72	Timed Release	(NOT ACTIVE)
74	Call Park	Allows the user to park a call on another telephone in the system.
75	Group Pickup	Allows the user to answer a call made to another set within the Pickup group.
76	Directed Pickup	Allows the user to answer any telephone that rings within the system.
77	Call Timer	Allows the user to see how long a call lasted.
78	Pause	Allows the user to insert a pause during a dialing sequence.
79	Exclusive Hold	Allows the user to put a call on hold at the current telephone. All appearances of the call on other telephones indicate the line is busy.
*80	Ring Volume	Allows the user to increase or decrease the ring volume of their telephone.
82	Camp-on	Allows the user to transfer and park an external call to another telephone in the system.
83	Privacy Control	Allows the user to make a shared line private, or release a shared line from private control.
84	Line Redirection	Allows the user to redirect a line within the system.
85	Do Not Disturb	Allows the user to block incoming calls from ringing on the telephone.
86	Background music	Allows the user to play music provided by a background music source through the speaker on the telephone.
88	Voice Call Deny	Allows the user to turn off the voice call feature at their set.
*501	Language Choice	Allows the user to change the default language that displays on the set.
520 to 535	System Wide Call Appearance (1 to 16)	Non-intercom calls are automatically associated with an available SWCA when the call is answered or originated. Calls stay associated with the key for the duration of the call. Features that interact with this feature: Hold, telephone keys, outgoing and incoming calls.
800	Trunk Answer	Allows the user to answer a ringing call placed in a service mode.
801	Call Queuing	Allows the user to answer calls in order when several calls occur at once. Calls are presented in this order: incoming calls, callback calls, then camped calls
802	Group Listening	This feature opens the microphone on the set to allow a group of people to hear a call through the telephone speaker, but the user must talk to the caller through the handset.
803	Time	Displays the current time.

Table 187 Button Programming Feature settings

Set command	Feature	Description
804	Wait for Dialtone	Places a pause in a dialing string that holds the following digits until a dialtone is perceived on the line.
807	Ringing (Signal) Call	Enter 807 and an extension to directly ring another telephone inside the system. This is the same process as pressing an intercom key and dialing an extension.
808	Long tones	Allows the user to specify the type of tones dialed out.
811	Call Information	Allows the user to view information about a current call.
812	Call Log - View Information	Allows the user to view call log information.
813	Call Log - Manual	Allows the user to manually active call logging.
815	Call Logs Auto Bumping	Allows the user to manually remove the oldest log item.
818	Call Charge Indication	Allows the user to view the charges for a call.
819	ONN blocking	Allows the user to block the call information from the telephone for an outgoing call.
870	Service Mode Status	Allows the user to view the current service mode being used.
871	Ringing Service	Allows the user to change the ringing service schedule.
872	Restriction Service	Allows the user to change the restriction service schedule.
873	Routing Service	Allows the user to change the routing service schedule.
897	MCID	(Malicious Call Identification) Allows the user to query the system for information about a call within 25 seconds after the user hangs up, but before the caller hangs up.
904	ACD agent login/log out	Allows the user to log in or out of ACD (Attendant Condole Directory).
908	ACD agent make busy/ ready	Allows the user to indicate ready or busy status on ACD.
909	ACD queue status	Allows the user to view the status of queued calls on ACD.
980	Express Messaging	Allows the user to log directly into voice mail to leave a message.
981	Voice Mail Login	Opens your mailbox to play your messages and to access mailbox options.
982	Voice Mail Operator settings	Allows the user to set the parameters for the voice mail operator.
984	Call forward to voice mail	Forwards incoming calls to your mailbox. (Available for the Norstar Voice Mail interface only.)
985	Display voice mail DN	Displays the voice mail extension number.
986	Transfer to mailbox	Transfers calls to a mailbox on the CallPilot system.
987	Voice mail interrupt	Intercepts a caller who is listening to your mailbox greeting or leaving a message.

Glossary

A

absorb length

This setting determines how many of the digits in a destination code the system does not dial. You assign the Absorb Length under **Destination codes**. (Services/Telephony Services/Call Routing)

access code

A digit or group of digits that provide direction to the system as to how to route a call or access a feature, such as call park. The Access Codes heading also provides access to the line pool codes and carrier codes. (Services/Telephony Services/General Settings/ Access Codes). Destination codes are a form of access codes for routing services (Services/Telephony Services/Call Routing).

Address Resolution Protocol (ARP)

ARP is a protocol for mapping an IP address to a physical machine address that is recognized in the local network. The physical machine address is also known as a Media Access Control or MAC address. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

As an example, this protocol is used when the Business Communications Manager maps an IP address to an IP telephone.

alarm code

A number that appears on an alarm telephone display when the system detects a fault.

Analog Terminal Adapter (ATA)

The ATA connects analog telecommunication devices, such as fax machines, answering machines, and single line telephones, to a digital media bay module on the Business Communications Manager system.

answer button

This telephone button allows you to monitor activity that occurs on another telephone in the system by indicating incoming calls to the other telephone. For instance, an attendant with a telephone with answer buttons can see which telephones on the system are busy, and answer the incoming call, if necessary.

One telephone can have up to four Answer buttons. When you assign an Answer DN to a telephone, the system assigns an Answer button to that telephone.

answer DN

The internal or directory number (DN) of a telephone that is monitored by an Answer button. You can assign up to four Answer DNs to a telephone. (Services/Telephony Services/System DNs)

application

A computer program that performs a wide range of tasks. Examples of application programs include word processing packages, spreadsheet packages and accounting packages.

Application Program Interface (API)

An API is an interface used by an application program to make requests of the operating system or another application. Unlike the graphical user interface or command interface, which are direct user interfaces, the API is an interface to an operating system or a program.

asynchronous

A method of transmission where the time intervals between characters are not required to be equal. Signals are sourced from independent clocks with different frequencies and phase relationships. Start and stop bits may be added to coordinate character transfer.

autobumping

A feature that determines how the system handles new Call Log items when your Call Log is full. When Autobumping is on, the system deletes the oldest entry when there is a new log entry. If Autobumping is off, your system does not log calls when your log is full. This feature is set by the user at the telephone.

autodial button

A memory button that provides one-touch dialing of external or internal numbers or to access features.

autolog options

A feature that allows you to select the type of calls stored in your Call Log.You can log calls not answered, calls not answered at this telephone but answered in the system, all calls answered and not answered at this telephone, or no calls. This option is set under **User Preferences**. (Services/Telephony Services/System DNs)

Automatic Daylight Savings Time

A feature that switches the system to standard or daylight savings time at programmed times. This feature is set when you run the Quick Install Wizard and specify a time zone setting.

Automatic Dial

A feature that allows you to dial without having to lift the receiver or select a line. The telephone must have a prime line assigned to use this feature. This feature is activated under **User Preferences**. (Services/Telephony Services/System DNs)

Automatic Handsfree

This feature automatically puts the telephone in Handsfree mode when you make or answer a call. This feature is assigned under Capabilities. (Services/Telephony Services/ System DNs)

Auto Hold

A feature that automatically places an active call on hold when you select another line. This feature is assigned under Trunk/Line data. (Services/Telephony Services/Lines/VoIP lines and Physical lines)

automatic privacy

See Privacy.

Automatic Telephone Relocation

This feature maintains the personal and system programming on a telephone that gets moved to a different jack on the same system, providing no other telephone is plugged into the original jack first. This feature is set under Feature Settings. (Services/Telephony Services/General Settings)

auxiliary ringer

An external telephone ringer or bell which rings when a line or a telephone rings. You can program an auxiliary ringer to ring when the system is in a selected schedule. Enable the auxiliary ringer under Capabilities. (Services/Telephony Services/System DNs)

B

B channel (bearer channel)

This is an ISDN line channel which is used for voice or data transmission.

background music

A feature that plays music through the speaker of a telephone. This feature requires an external music source that is attached to the MSC on the Business Communications Manager. The feature is enabled under Feature settings. (Services/Telephony Services/ General Settings)

backup

This is a process, enabled through the BRU button on the Unified Manager, that allows you to copy all or specific data files from your Business Communications Manager system to a file that can be transferred to a secure place in case of system problems that would require the Business Communications Manager to be re-initialized.

base station

This device is part of the wireless handset systems that can be used with the Business Communications Manager. It contains radios that receive and send signals to a cordless handset used within a specific radius of the base station. The base station connects to a media bay module installed in your Business Communications Manager System. This allows you to provide communication mobility from your system.

Basic Rate Interface (BRI)

An ISDN interface that uses two B channels and a D channel (2B+D). ETSI BRI is the European Telecommunications Standards Institute specification for BRI ISDN service.

baud rate

A unit of measurement of data transmission speed through a media channel, such as a modem. Baud rate is approximately equivalent to Bits Per Second (BPS).

bearer channel

See B channel.

Basic Input Output System (BIOS)

A program contained in Read Only Memory (ROM) that acts as the interface between software programs and the computer hardware.

bit

An abbreviation for Binary Digit. A bit is the smallest unit of information identified by the computer. A bit has one of two values, 0 or 1, to indicate off or on.

bit error rate test

A test that checks the transmission of data across the voice and data channels between the system and any telephone.

BPS (Bits Per Second)

The speed of data transmission between two computers.

bus

A collection of communication lines that carry electronic signals between components in the system. On your Business Communications Manager MSC, buses are also referred to as DS30 channels. Besides internal communications, the Business Communications Manager MSC uses buses to support media bay modules and IP telephony components.

busy lamp field (BLF)

This is the display field beside the buttons on the telephones that displays an arrow indicator when the button is in use.

byte

The amount of space required to store a single character. One byte is equal to eight bits.

C

Call Duration Timer

A feature that allows you to check how long you were on your last call or how long you have been on your present call. (✆ 7 7)

- no active call: set displays the duration of the last active call
- active call: set displays elapsed time of call (not dynamic)

Call Forward

A feature that forwards all the calls arriving at your telephone to another telephone in your system, or, if you are using ISDN lines to forward the call, to external systems. To have calls forwarded outside the system on other types of lines, use the line redirection feature. Call forward is configured under Capabilities. (Services/Telephony Services/System DNs)

- Call Forward No Answer: forwards all calls if the original target telephone is not answered. The system transfers the calls after a specific number of rings.
- Call Forward On Busy: forwards all calls if the target telephone rings busy.
- Call Forward Override: allows you to override call forward directed at your telephone, and ask the user to stop forwarding calls to you.

call information

This feature allows you to display information about incoming calls. For external calls, you can display the name of the caller, telephone number, and line name. For an internal call, you can display the name of the caller and the internal number of their telephone. You can receive information about ringing, answered, or held calls. (✆ 8 1 3)

call log

If call log is active on a telephone, the use can view a record of incoming calls. (✆ 8 1 2)
The log can contain the following information for every call:

- sequence number in the Call Log
- name and number of caller
- long distance indication
- call answered indication
- time and date of the call
- number of repeated calls from the same source
- name of the line that the call came in on.

See Autobumping and Autolog options for more information.

Call Park

This feature allows you to place a call on hold so that another user can retrieve it from another telephone in the system. The user retrieves the call by selecting an internal line and entering a retrieval code.

The retrieval code appears on the display of your telephone when you park the call. You can park up to 25 calls on the system at one time. (74)

You can also specify a prefix to the retrieval under Access codes. (Services/Telephony Services/General Settings)

call park callback

See Callback.

Call Park Prefix

The first digit of the retrieval code of a parked call.
This digit cannot conflict with:

- the first digit of any existing extension number
- line pool access codes
- the direct-dial digit
- the external line access or destination code

The default Call Park prefix digit is 1. To disable Call Park, set the Call Park prefix to none. Assign the Call Park prefix under Access codes. (Services/Telephony Services/ General Settings)

call pickup directed

This feature allows you to answer a call ringing at any telephone by entering the internal number of that telephone. (7 6 + DN)

call pickup group

See Pickup Group.

Call Queuing

If you have several calls waiting at your telephone, you can activate the Call Queuing feature to answer the calls in order of priority.

The order of priority is: incoming calls, callback calls, and camped calls. (8 0 1)

Callback

If you park, camp, or transfer a call to another telephone and no one answers the call, the call rings again at your telephone. Set the timing for this in Timers/Transfer callback timeout. (Services/Telephony Services/General Settings)

Camp-on

A feature that allows you to reroute a call to a telephone when all the lines on that telephone are busy. To answer a camped call, use Call Queuing or select a line if the camped call appears on your telephone. Queued calls get priority over camped calls.

MCDN: On an MCDN network, the central attendant can camp calls on any telephone in the network.

Camp Timeout

The length of a delay before a camped call returns to the telephone that camped the call. Set the length of delay under Timers. (Services/Telephony Services/General Settings)

central answering position (CAP) module

This 48-button module connects to an M7324 telephone to provide additional answer buttons. You can connect a maximum of two CAP modules to a single M7324 telephone. CAP configuration. You can have a maximum of five telephones set up with CAP in a system. Configure the modules under CAP assignment. (Services/Telephony Services/ General Settings)

Challenge-Handshake Authentication Protocol (CHAP)

CHAP is a method of establishing security on PPP links where the peers must share a plain text identifier. The caller sends a challenge message to its receiving peer and the receiver responds with a value it calculates based on the identifier. The first peer then matches the response with its own calculation. If the values match, the link is established.

CHAP is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP).

Channel Service Unit (CSU)

A device on the digit trunk interface (DTI) that is the termination point of the T1 lines from the T1 service provider. The CSU collects statistics on the quality of the T1 signal. The CSU ensures network compliance with FCC rules and protects the network from harmful signals or voltages.

Class of Service (COS) password

COS defines the set of features and lines available to the user for a call into the Business Communications Manager system. The COS password determines which restriction filters and remote access packages are active when the caller uses a specific password. Callers accessing the system from outside the system can change the Class of Service for a call by entering a six-digit Class of Service password. However, internal users cannot change their access to features with a COS password, only their restriction filters. Assign this feature under COS Passwords. (Services/Telephony Services/General Settings)

client

A client is a computer system or process that requests a service of another computer system or process. For example, a workstation requesting the contents of a file from a file server is a client of the file server.

cold start

A cold start occurs when you lose all system programming.You can lose system programming after a major event such as an extended power failure. If this occurs, you will need to restore the data to your system from your backup files.

conference

A feature that allows you to establish a three-person call at your telephone. (flash 3 or the conference/transfer button on the telephone)

configuration

See programming.

Coordinated Dialing Plan (CDP)

In this configuration, networked sites are viewed as independent nodes in that each site has a range of extension numbers (i.e. 2221-2267), plus a unique prefix number. Example: Site one = prefix 10, therefore you would dial numbers from 102221 to 1022267 to reach that network. Site two = prefix 20, therefore, you would dial numbers from 202221 to 2022267 to reach that network. See also, Universal Dialing Plan. Set the specifications for CDP under Dialing plan/Private network. (Services/Telephony Services/General Settings)

D

D channel (data channel)

A transmission channel which is packet-switched. It is used for call setup, signaling and data transmission.

data link connection indentifier (DLCI)

The DLCI is used to identify a permanent virtual circuit (PVC) in frame relay networks.

DECT (digital enhanced cordless telecommunications

This cordless protocol provides localized mobility services to the Business Communication Manager through a DECT media bay module. This service is region-specific.

defaults

The settings for all features when you first install the system. You change the settings from their defaults in programming. Defaults are determined by which region and which telephony template you choose when you first install your system. (Quick Start Wizard)

Delayed Ring Transfer to Prime

DRT allows the system to transfer an unanswered call on an external line to the prime telephone related to that line if the targeted telephone is not answered within the configured number of rings. Configure this setting under Feature settings/Delayed Ringer Transfer. (Services/Telephony Services/General Settings)

destination code

A two to seven-digit number that the system reads and translates into the digits that are dialed out. This code must not conflict with any other access code on the system. Assign destination codes in Destination Codes. (Services/Telephony Services/Call Routing)

dial-up connection

A dial-up connection is a temporary connection between computers that is established over an analog or digital telephone line.

dialing restriction

See Restriction filter.

Differentiated Services (DiffServ)

DiffServ is a method of implementing QoS service for IP networks. DiffServ is intended to improve network performance. Instead of applying faster, more advanced technology, networks are managed by appropriate network policies. With DiffServ there is a cost associated with higher quality services, and a risk with lower quality services.

Digital Access Signaling System Number 2 (DASS2)

A UK proprietary standard for signaling on ISDN connections between customer premises and the public network. DASS2 is used between the customer equipment and ISDN local exchange and is suitable for multiple access.

Digital Private Network Signalling System (DPNSS)

DPNSS is a networking protocol that provides access to Business Communications Manager features over multiple combined networks. Corporate offices, separated geographically, can be linked over DPNSS to other Business Communications Manager systems, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Business Communications Manager systems to function like a private network. DPNSS is available in International systems only.

direct-dial

This feature allows you to dial an assigned telephone in your system with a single digit. You can assign as many as five direct dial telephones in a system. These telephones are configured under the Direct Dial heading (Services/Telephony Services/General Settings).

Each telephone in the system has one direct-dial telephone. Each telephone can be assigned a direct-dial set under Capabilities. (Services/Telephony Services/System DNs).

Direct-dial #

This is a single, system-wide digit for calling the assigned direct-dial telephone of any telephone. This digit is defined under Access codes. (Services/Telephony Services/ General settings)

directed pickup

See Call Pickup Directed.

directory number (DN)

A unique number that the Business Communications Manager system assigns to every telephone or data terminal. You use the DN to identify a telephone for the Business Communications Manager configurations that require specific telephone connections.

disconnect supervision

This line setting enables the system to detect if an external caller hangs up. After an external caller hangs up, the system disconnects the line. Disconnect supervision is defined under the module settings for the lines. (Resources/Media Bay Modules)

disk drive

A mass storage device that searches, reads and writes data on a disk.

display

A one or two line screen on a Business Communications Manager telephone that shows commands and options for that telephone.

display buttons

The three buttons that appear below the display on a Business Communications Manager telephone.

display options

The options available to a user. These options appear on the telephone display. Select the options on the display using the display buttons. Enter information from the dialpad.

Distinctive Ring

In system programming, this feature allows you to define a distinct ring for different types of calls, to provide a priority system for incoming calls.

As a feature, the user can choose a specific ring type for incoming calls.

DNS proxy

A Domain Name Service (DNS) proxy translates alphabetic domain names into computer-readable IP addresses. For example, the domain name www.nortelnetworks.com for the Nortel Networks web site can translate to the IP address 192.177.5.18. After a domain name is translated into an IP address, the workstations on your network can communicate with the web site. Depending on the configuration of your system, you can let your workstations know that Business Communications Manager is the DNS proxy.

Do Not Disturb

The DND feature stops calls from ringing at your telephone. Only Priority Calls will override this feature and ring at your telephone. A line button flashes when you receive a call, but the call does not ring. (✆ 8 6) You can set the telephone to send this signal automatically through a setting in Capabilities. (Services/Telephony Services/System DNs)

domain name

The domain name is used to organize Internet names into manageable groups, such as nortelnetworks.com, where nortelnetworks is the domain name.

Domain Name Server (DNS)

The domain name system or domain name server is the system in the Internet that maps names of objects, most usually host names, into IP numbers or other resource record values. The name space of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain.

driver (device)

A program that allows a hardware peripheral, such as a network interface card, to communicate with the Business Communications Manager.

dual tone multifrequency

DTMF provides two distinct telephone signaling tones used for dialing.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a protocol that allows network administrators to centrally manage and automate the assignment of IP addresses in an network. When an organization sets up its computer users with a connection to the internet, internet protocols (TCP/IP) demands that an IP address must be assigned to each machine as well as to any device connected to the network.

Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP allows the network administrator to supervise and distribute IP addresses from a central point. It also automatically sends a new IP address when a computer is plugged into a different place in the network.

dynamic IP address

Dynamic IP addresses are assigned to computers by an IP address server, as the computer needs it. Usually there is a particular range or scope of IP addresses that your network uses. With dynamic IP addressing, a computer can have a different IP address every time it connects to the network. Other devices must know the IP address of the computer so they can communicate with it. The IP address server manages the assignment of IP addresses to the client workstations. See also static IP address.

E

Emergency 911 dialing

The ability to access a public emergency response system by dialing 911. State and local requirements for support of Emergency 911 Dialing service by Customer Premises Equipment vary. Ask your local telecommunications service provider about compliance with applicable laws and regulations. Note, there are special restrictions about setting up this service on IP telephones that are connected to the Business Communications Manager.

emergency telephone

A single-line telephone, also referred to as a 500/2500 telephone, that becomes active when there is no power to the Business Communications Manager.

ethernet

A Local Area Network (LAN) protocol that is the original Carrier Sense Multiple Access/ Collision Detect (CSMA/CD) LAN that allows computers, and Business Communications Managers to listen for pauses before they communicate. Ethernet LANs use coaxial cable or twisted pair wiring to connect network equipment.

event message

The system stores event messages in the system log and displays these messages during a maintenance session. They record many different events and activities in the system.

exceptions

See Overrides.

Extended Data-Out (EDO)

Extended Data-Out (EDO) is a type of Dynamic Random Access Memory (RAM) where storing data to and reading data from the memory is faster.

external code

The number you dial to access a line outside of your Business Communications Manager system. For instance, the external code to access the public network is set to a default of 9.

These codes are defined under Access codes (Services/Telephony Services/General Settings) and Destination codes (Services/Telephony Services/Call Routing). You also use an external code to support the T7100 telephone and single-line telephones connected to an Analog Terminal Adapter (ATA2).

external paging

Use this feature to make voice announcements over an externally-installed loudspeaker connected to the Business Communications Manager through the MSC.

F

FAX

FAX works with Business Communications Manager Voice Messaging. FAX allows a caller to send a fax document to a voice mailbox.

feature code

This is a code that is entered at a telephone to activate a feature.

filtering

Filtering is the process of examining a data packet on the network to determine the destination of the data and whether the packet should be passed along on the local LAN, copied to another LAN, or dropped.

frame

A frame is a unit of data transmission in a local area network.

frame relay

A frame relay is a high-speed, packet switching WAN protocol designed to provide efficient, high-speed frame or packet transmission with minimum delay. Frame relay uses minimal error detection and relies on higher level protocols for error control.

FTP

The file transfer protocol (FTP) allows a user on one host to access and transfer files to and from another host over a network. On the Internet, FTP refers to a tool for accessing linked files.

full autohold (on idle line)

When this feature is on, Full Autohold automatically puts the current line on hold when you select another line. Enable Full Autohold under Line XXX/Trunk Line Data. (Services/Telephony Services/Lines)

You can also define auto hold for each telephone, in this case, it applies to any incoming calls. Define auto hold for each telephone under DN XXX/Capabilities. (Services/Telephony Services/System DNs)

A user can also override the system auto hold setting using [⎋] [7] [3]

Fully Qualified Domain Name (FQDN)

The combination of host name and domain name. For example, mycomputer.nortelnetworks.com is a Fully Qualified Domain Name.

G

gateway

A system that links two different types of networks and enables them to communicate with each other. Business Communications Manager is the gateway that links your network to the intranet or internet. Depending on your configuration, you can let your workstations know that Business Communications Manager is your Internet gateway.

ground start trunk

Ground start trunks provide the same features as loop start trunks. Use this type of trunk when the local service provider does not support disconnect supervision for the digital loop start trunks. By configuring lines as ground start, the system can identify when a caller hangs up the telephone at the far end. Ground start trunks are available only on a Digital Trunk Interface module (DTM).

group listening

This feature allows you to have other people in your office hear a caller through your telephone speaker. The caller hears you when you speak into the receiver and cannot hear other people in the office. (e 8 O 2)

You can cancel Group Listen for the current call. Group Listen cancels automatically when you hang up the Group Listen call.

H

H.323

H.323 is the standard for using IP to send voice and video within intranets and on the public Internet.

handsfree

A feature you can use to make calls through your telephone without lifting the telephone receiver. Activate Full Handsfree under Capabilities (Services/Telephony Services/System DNs). When you activate handsfree, Business Communications Manager assigns a Handsfree/Mute button to the telephone.

handsfree (HF) answerback

This feature automatically turns on the microphone at a telephone that receives a Voice Call so that the person receiving the call can respond without lifting the receiver. Activate Handsfree Answerback under Capabilities (Services/Telephony Services/System DNs).

hard disk

A data storage device that uses rigid magnetic disks permanently installed inside the computer CPU or a portable unit.

held (line) reminder

A telephone rings and displays the message `On hold: LINENAM` when you place an external call on hold for programmed period of time. Set the Held Line Reminder under Feature settings. (Services/Telephony Services/General Settings).

High-level Data Link Control (HDLC)

HDLC is a group of protocols or rules for transmitting data between network points or nodes. Data is organized into a unit, called a frame, and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent. HDLC is one of the most commonly-used protocols in Layer 2 of the industry communication reference model, Open Systems Interconnection (OSI).

Hold button

Use this button to interrupt calls so that you can perform another task without disconnecting the caller.

Hook Switch Flash

See Link.

Host Name

In networking, this is the name of a computer that provides services, such as database access, to other computers or Business Communications Managers in the domain. Computers with a host name also have a unique IP address. Because the Business Communications Manager has a unique IP address, the Business Communications Manager qualifies as a host.

Host system signaling

Also referred to as end-to-end signaling. Telephones can access a remote system or dial a number on an different carrier by using host feature activation codes, such as Link, Pause and Run/Stop.

Hotline

This feature automatically calls a pre-assigned number when you lift the telephone receiver or press the Handsfree/Mute button. A Hotline number can be an internal or external number. Assign Hotline under Capabilities/Hotline. (Services/Telephony Services/System DNs)

HTTP proxy

See Web proxy.

I

ICMP

ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams, however, the messages are processed by the TCP/IP software and are not directly apparent to the application user.

In-band

In-band is a method of device access that utilizes a network interface component within the device.

Integrated Services Digital Network (ISDN)

A digital telephone service that allows for a combination voice and data connection over a single, high-speed connection. ISDN service can operate over the same copper twisted-pair telephone line as analog telephone service. The Business Communications Manager uses two versions of ISDN, BRI and PRI.

Intercom button

A button that provides access to internal lines within a Business Communications Manager system. These buttons can also provides access to external lines by adding an access or destination code to the internal line number. You can assign a telephone a maximum of eight intercom buttons, although not all buttons will display, depending on the style of telephone. Configure intercom (I/C) buttons under DN XXX/Line Access. (Services/Telephony Services/System DN)

intercom keys

See intercom button.

internal line

A line on your telephone dedicated to making calls to destinations inside your Business Communications Manager. An internal line can connect you with an external caller if you use it to access a line or line pool. You can direct internal lines to specific telephones or groups of telephones using target lines.

internal number

A number, referred to in Unified Manager as a Directory Number (DN), which identifies a telephone or device assigned to the Business Communications Manager.

internal user

A person using a telephone connected to the Business Communications Manager telephone.

Internet

A global TCP/IP network linking millions of computers for communications purposes.

Internet Engineering Task Force (IETF)

The IETF is the committee that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society's Internet Architecture Board (IAB).

Internet-standard Network Management Framework

Device configuration and monitoring via SNMP.

IP

The Internet Protocol (IP) is the protocol that supports data being sent from one computer to another on the Internet. Each computer on the Internet has at least one address that uniquely identifies it from all other computers on the Internet. When you send or receive data, the message gets divided into units called packets. Each of these packets contains the Internet address of the sender and the receiver.

IP is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

IP address

The Internet Protocol address is a unique identifier that allows communication over the Internet to be directed to the appropriate destination. Every computer on the Internet must have a unique IP address. IP addresses are allocated by an Internet service provider (ISP) in the following format: nnn.nnn.nnn.nnn, where nnn is a numeric value from 0 to 255. IP addressing might be referred to as being a static IP address or a dynamic IP address.

IPX

IPX (Internetwork Packet Exchange) is a networking protocol from Novell that interconnects networks that use Novell NetWare clients and servers. IPX is a datagram or packet protocol. IPX works at the network layer of communication protocols and is connectionless (that is, it doesn't require that a connection be maintained during an exchange of packets as, for example, a regular voice phone call does).

Interrupt Request (IRQ)

IRQ is a signal that is sent by a hardware device to the microprocessor, requesting its immediate attention. For example, every communications port has an interrupt request line for telling the microprocessor when data is received or transmitted.

IRQ Conflict

An IRQ conflict occurs when two hardware devices have the same IRQ. When an IRQ conflict occurs, the user must configure the IRQ settings to solve the conflict.

K

Kbyte

The abbreviation for kilobyte. A kilobyte is equal to 1024 bytes.

keycode

This code is used to enable application options on the Business Communications Manager. These codes are entered by the installer or system administrator. Keycodes are a combination of access codes that are encrypted to open a single application on a specific Business Communications Manager.

L

Last Number Redial

This feature allows you to redial the last external number you dialed. (✆ 5)

Least cost routing

See Routing service.

line

The complete path of a voice or data connection between one telephone, or other device, and another.

line number

A number that identifies an external line connected to the Business Communications Manager. The total number of lines depends on the number and type of trunk media bay modules installed. Voice over IP (VoIP) trunks and target lines are also defined as line numbers, although they do not connect to the system through physical lines.

line pool

A group of lines used for making external calls. Line pools provide an efficient way of giving a group of users access to a group external lines using one line button. This also provides cost saving because you can assign a greater number of telephones to fewer lines, depending on your system traffic rates. Assign a line to be part of a line pool under Trunk/ Line data. (Services/Telephony Services/Lines/Physical lines orVoIP lines)

Line Redirection

This feature allows you to redirect all calls from an incoming line, usually to a destination outside the system. After you redirect a line, you cannot answer the line within the system. (✆ 8 4)

You enable the service and set up redirect ring under Capabilities. (Services/Telephony Services/System DNs)

This feature differs from Call Forward in that Call Forward redirects calls coming in on all lines to another destination, such as voice mail, while Line Redirection redirects only the specific line.

Link

If you connect the Business Communications Manager system to a Private Branch Exchange (PBX), you can use a Link signal to access special features. You can include the Link signal as part of a longer stored sequence on an External Autodial button or in a Speed Dial code. The Link symbol uses two of the 24 spaces in a dialing sequence.

Local Area Network (LAN)

A group of computers or Business Communications Managers connected so they can communicate and work together.

Long Tones

This feature allows you to control the length of a tone so that you can signal devices such as fax or answering machines. These devices require tones longer than the standard 120 milliseconds. (✆ 8 O 8)

M

Media Access Control (MAC)

This is a physical address that is the portion of the data-link layer in 802.x networks.It controls addressing information of the packet and enables data to be sent and received across a local area network. IP telephones, for instance, have a MAC address that allows the Business Communications Manager to keep track of individual telephones even if dynamic IP addresses are used.

mailbox

A storage place for voice messages on Business Communications Manager Voice Messaging.

MCDN

Although defined as a Meridian Customer-Defined Network, this network protocol provides Meridian system features to Business Communications Manager systems that are network to the Meridian over PRI SL-1 lines, providing the MCDN keycode has been entered at the Business Communication Manager. There are setup requirements from both ends of this network link to properly enable the features.

media channel

Media channels are the communication channels used to send voice and data information between the devices and feature ports. Media channels are also known as B channels. The Business Communications Manager uses the MSC to manage these channels on the system.

Meridian 1 ISDN Primary Rate Interface

A protocol used between members of the Nortel Networks Meridian family of Private Telecommunication Network Exchanges. The signaling information is carried via time slot 16 of a 2.048 Mbit/s digital transmission system.

MHz

The abbreviation for megahertz, which is a unit of measure indicating frequency in millions of cycles per second.

microprocessor

An electronic component that is the center of all activity inside the Business Communications Manager. The microprocessor controls the operation of the computer and is responsible for executing program commands. A microprocessor is also referred to as the Central Processing Unit (CPU).

modem

A communications device that allows computers to exchange data over telephone lines. A modem uses electronic processes called modulation and demodulation. The modem changes (modulates) the data into tones to send to another modem and converts (demodulates) tones when receiving from another modem.

Move Line

This feature allows you to move external lines assigned to your telephone to different buttons on your telephone.

Multilink PPP

Multilink PPP is an extension to the PPP protocol that enables you to group a set of links into a bundle for more bandwidth. The links in the bundle can operate at different speeds. Typical links can be ISDN B channels, dial-up connections, and leased-lines.

music source

You can connect a radio or other source of music to the system to provide music for the Music on Hold and Background Music features. A music source is customer-supplied. The source is connected through a jack on the MSC on the Business Communications Manager.

N

NetBIOS

The Network Basic Input/Output System (NetBIOS) is an interface and upper-level protocol developed by IBM for use with a proprietary adapter for its PC network product. NetBIOS provides a standard interface to the lower networking layers. The protocol provides higher-level programs with access to the network. Windows NT systems use NetBIOS.

network

Two or more computers linked electronically to share programs and exchange data. This process requires both hardware devices and software to coordinate the connection and data exchange.

network device

A network device is a hardware device used as a communications component within a network.

network DN

A number supplied by the ISDN network service provider for ISDN terminal equipment.

Network Interface Card (NIC)

A network interface card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network. Personal computers and workstations on local area networks (LANs) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet or Token Ring. Network interface cards provide a dedicated, full-time connection to a network.

O

On Hold

A setting that controls what external callers hear: music, tones, or silence, when you place the call on hold. Configure this setting under Feature settings. (Services/Telephony Services/General settings)

Open Shortest Path First (OSPF)

A routing protocol used within larger autonomous and complex networks in preference to the Routing Information Protocol (RIP) which suits a small network. Like RIP, OSPF is designated by the Internet Engineering Task Force as one of several Interior Gateway Protocols.

out-of-band

Out-of-band is a method of device access which circumvents the network interface components within the device.

overflow

For digital and IP telephones, turn this setting on to allow the system to choose a fallback path for an outgoing call.

The feature is turned on under Routing Service/<schedule>. (Services/Telephony Services/Scheduled Services). You also need to set up routes and schedules that provide the correct routing for the normal and fallback lines.

overrides

One component of a restriction filter. Overrides are numbers you can dial when they are not allowed by a more general restriction. Enter these numbers under Overrides for each restriction within specific filters. (Services/Telephony Services/Restrictions filters/ Filter XX/Restrictions)

P

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file, such as an e-mail message, HTML file, GIF file, URL request, and so forth, is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into pieces of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When the packets have all arrived, they are reassembled into the original file.

A packet switching scheme is an efficient way to handle transmissions on a connectionless network such as the Internet. An alternative scheme, circuit switching, is used for networks allocated for voice connections. In circuit switching, lines in the network are shared among many users as with packet switching, but each connection requires the dedication of a particular path for the duration of the connection.

Packet and *datagram* are similar in meaning. A protocol similar to TCP, the User Datagram Protocol (UDP) uses the term datagram.

Page

Use this feature to make announcements over the Business Communications Manager system. You can make page announcements over the telephone speakers and/or external speakers.

- Page tone is defined under Feature settings. (Services/Telephony Services/General Settings)
- Page Time out is defined under Timers (Services/Telephony Services/General Settings). This setting controls how long a Page Announcement can last.
- Page zone defines An area in the office that receives internal page announcements that other areas of the office do not hear. This feature is defined for each telephone under Capabilities. (Services/Telephony Services/System DNs)

Password Authentication Protocol (PAP)

This is a procedure used by PPP servers to validate a connection request. PAP works as follows:

1. After the link is established, the requestor sends a password and an ID to the server.
2. The server either validates the request and sends back an acknowledgement, terminates the connection, or offers the requestor another chance.

Passwords are sent without security and the originator can make repeated attempts to gain access. For these reasons, a server that supports CHAP will offer to use that protocol before using PAP.

Park prefix

See Call park prefix.

Park timeout

The time before an unanswered parked call returns to the telephone that parked it. Set this feature in Timers. (Services/Telephony Services/General settings)

Peripheral Component Interconnect (PCI) Slot

These are hardware sockets on a circuit board. For instance, the Business Communications Manager has four PCI slots on the MSC board. Each slot contains one PCI III card, which handles call processing for the system.

Permanent virtual circuit (PVC)

The PVC is an end-to-end virtual connection in frame relay networks.

Personal Speed Dial

These are two-digit codes between 71 and 94 that are assigned to specific telephones to dial external numbers with just one button press. Configure speed dials under User Preferences/User speed dials/Speed dial #XX. (Services/Telephony Services/System DNs

Pickup Group

You can place a telephone into one of nine call pickup groups. You can pick up a call ringing at a telephone within a pickup group from any telephone within the same pickup group. Assign a telephone to a pickup group under Capabilities. (Services/Telephony Services/System DNs)

pin-1

An indicator on the first pin on an electronic component. You use this indicator to help you correctly align the component when attaching or installing it.

Point-to-point protocol (PPP)

PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connected to a server by a telephone line. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair, fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

pool

See Line pool.

port

A connector on the Business Communications Manager that allows data exchange with external devices, such as external page or music equipment or a serial cable connection to a computer.

portable telephone

See Companion portable telephone and DECT

power cable

A cable that connects the Business Communications Manager to a power source.

pre-dial

A feature that allows you to enter a number and check it on your telephone display before you list the handset or select a line. The Business Communications Manager system dials the number when you lift the receiver or select a line.

Primary Rate Interface (PRI)

An ISDN interface that uses 23 B channels and a D channel (23B+D).

Prime line

The line the system selects for your telephone when you lift the receiver, press the Handsfree/Mute button or use an external dialing feature. Assign a Prime Line to a telephone under Line access. The default is the intercom button (I/C). (Services/Telephony Services/System DNs)

Prime Set (prime telephone)

A telephone that provides backup answering for incoming calls on external lines. The prime telephone for a line will ring for any unanswered calls on that line. Assign a prime telephone to a line under Line XXX/Trunk Line data. (Services/Telephony Services/ Lines).

Priority Call

If you get a busy signal when you call a person in your office, you can interrupt that person for an urgent call. Enable this feature for a telephone under Capabilities. Set the intrusion level, which defines who can interrupt calls and whom you can interrupt under Capabilities/Intrusion. (Services/Telephony Services/System DNs). (✆ 6 9)

Privacy

This feature determines if a system user can select a line in use at another telephone and join an established call. Auto Privacy can be enabled under Line XX/Trunk Line data. Users can turn this feature on and off during separate calls. (✆ 8 3)

Private branch exchange (PBX)

A PBX is a small telephone system connected to a central office (CO), but which is owned and operated privately. An example of a PBX system is the Meridian 1 system. The PBX can connect directly to telephones or pass lines on to another private telephone system, such as a Business Communications Manager.

private line

See Private to.

private network

A telephone network of PBXes and/or key service units (KSU) connected through dedicated trunks or voice over IP (VoIP) trunks.

Private to

This feature allows you to select the telephone that exclusively uses a line. The line cannot appear on another telephone, except the prime telephone for that line. You cannot place private lines into line pools. Private lines are assigned under Line XXX/Trunk Line data/ Line Type. (Services/Telephony Services/Lines)

programming

Setting the way the Business Communications Manager system works. Programming includes system-wide settings and separate telephone and line settings.

protocol

A set of rules and procedures for exchanging data between computers or Business Communications Managers on a network or through the Internet.

proxy

A proxy is a server that acts on behalf of another.

public line

An external line that you can assign to any telephone or to many telephones on a system. Assign a line as public under Line XXX/Trunk Line data/Line Type. (Services/Telephony Services/Lines)

public network

The central office telephone network that provides trunks and lines to individual telephone users and private systems.

pulse/tone dialing

An external line setting for pulse or tone dialing. Pulse is the traditional method of dialing used by rotary-dial or push-button single-line telephones. Tone dialing allows telephones to communicate with other devices such as answering machines.You require tone dialing to access the features that PBX systems can provide or to use another system remotely.

Q

Quality of Service (QoS)

On the Internet and in other networks, QoS refers to guaranteed throughput level. QoS allows a server to measure, improve and, to some level, guarantee the transmission rates, error rates, and other data transmission characteristics. QoS is critical for the continuous and real-time transmission of video and multimedia information which use high bandwidth.

Q reference point signaling (QSIG)

QSIG is an ETSI (International) standard signaling for multi-vendor peer-to-peer communications between PBXs and/or central offices.

R

RAM (Random Access Memory)

Computer memory that stores data temporarily. RAM stores the data used by the microprocessor as it executes instructions. The contents of RAM are erased when you restart or turn off the Business Communications Manager.

recall

See Link.

receiver

The handset of a telephone.

Regression Code

This feature restores the previous system security number so that previously applied UTAM Activation Codes and Portable Credit Codes can be re-entered to restore full system operation for Companion components. Also required in cases of system recovery. You cannot use this code again.

relaying

Relaying is the process of moving data along a path determined by a routing process. The data is relayed between a source and a destination.

Remind delay

A feature, referred to as Held Line Reminder, causes a telephone to beep and display the message `On hold: LINENAM` when a call has been on hold for a programmable period of time. Turn the feature on and set the timing under Feature settings. (Services/Telephony Services/General settings)

remote access

The ability to dial into a Business Communications Manager system from outside the system and use selected features. The Class of Service determines which lines, features, and dialing capabilities are available.

remote access dial restriction

See Remote restriction.

Remote access service (RAS)

The RAS is the ability to get access to a computer or a network from a remote distance. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporate network. Home users get access to the Internet through remote access to an Internet service provider (ISP).

A remote access server is the computer and associated software that is set up to handle users seeking access to the network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

remote device

A remote device is any network device that is accessible only by means of communication over a digital or analog (dial-up) network.

remote monitoring

A feature that allows an off-site technician with a computer to call in and troubleshoot your system through the built-in modem.

remote paging

This feature allows remote users to use the system paging feature. Access to this feature is governed by the Class of Service for the call.

remote access package

A restriction filter that is applied to an incoming line to control which digits are dialed during an incoming remote access call. Remote access packages are defined under Remote Access packages (Services/Telephony Services/General Settings), and assigned under COS Passwords (Services/Telephony Services/General Settings)

remote user

Someone who calls into a Business Communications Manager system from a telephone outside that system and uses system features or lines. See Remote Access.

restriction filter

Restriction filters are configured to prevent some telephone numbers or feature codes from being dialed. Restriction filters can be applied to lines, sets, specific lines on a set, and to Class of Service passwords. Under restriction filters, you can enter override numbers that you want to circumvent the general restrictions. Configure filters under Restriction filters. (Services/Telephony Services)

restriction service

You can assign alternative dialing filters to lines, telephones, lines on a particular telephone, and alternative remote filters to lines at specified times of the day and on specified days. Set up restriction schedules under Restriction service. (Services/Telephony Services/Scheduled Services)

restrictions

Restrictions are numbers you cannot dial when that dialing filter is in effect. You can use ⌂68 to override restrictions for a line to make a call.

Ring Again

Ring Again instructs the system to tell you when a currently busy telephony hangs up or when an unanswered telephone is being used. (⌂2)

ring group

Ring groups allow you to program a specific group of telephones to ring during a scheduled time, for specific lines. You can program a maximum of 20 ring groups.

Configure ring groups under Ringing service. (Services/Telephony Services/Scheduled Services)

ring type

A feature that allows you to select one of four distinctive rings for your telephone. See also distinctive ring. This feature is set under User Preferences, but can be changed at a telephone. (Services/Telephony Services/System DNs)

ring volume

A feature that allows you to set the volume at which your telephone rings. This is a telephone feature and has no system setting.

ringing service

A Services section that allows you to make additional telephones ring at specified times of the day and on specified days. Refer to ring group.

RIs button

Ends a call in the same way that hanging up the receiver does.

ROM (Read Only Memory)

Memory that stores data permanently. ROM contains instructions that the Business Communications Manager needs to operate. The instructions stored in ROM cannot be changed and are used by the Business Communications Manager each time it is turned on or restarted.

router

A router is a device that forwards traffic between networks, based on network layer information and routing tables. A router decides which path network traffic follows using routing protocols to gain information about the network and algorithms to choose the best route based on a routing matrix.

routing

The path a message takes from its origin to its destination on a network or the Internet. Configure routing under Call Routing. (Services/Telephony Services)

Routing Information Protocol (RIP)

RIP enables routers in the same autonomous system to exchange routing information by means of periodic updates. RIP is a widely-used protocol for managing routing information within a self-contained network such as a corporate local area network (LAN) or an interconnected group of such LANs.

Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts is has on record) to its closest neighbor host every 30 seconds. The neighbor host passes the information to its next neighbor and so on until all hosts within the network have the same routing path information, a state known as network convergence. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.

RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds may put a heavy amount of extra traffic in the network.

The major alternative to RIP is the Open Shortest Path First Protocol (OSPF).

routing service

Routing services defines schedules that allow you to change the route of a call without changing the destination code. This provides a way of shifting from one service provider to another at different times of the day if the rates are better. The system determines the routing; the user continues to dial the same number. Use Routing services to configure these schedules. (Services/Telephony Services/Scheduled Services)

Run/Stop

A feature that creates a break point in a programmed external dialing sequence. When you press a programmed key, the system dials the number up to the run/stop. When you press the programmed key again, the system dials the digits following the run/stop.

S

Saved Number Redial

A feature that allows you to save the number of the external call you are on, providing you dialed the call, so that you can call it again later.

schedules

Any of six sets of services you can apply to your system. See Services.

selective line redirection

See Line Redirection.

serial port

A port that sends and receives data one bit at a time. You can use this port to connect the Business Communications Manager to a printer, external modem or mouse. The serial port connector has nine pins and is identified by software with the letters COM and a single digit, such as COM1.

Service modes

See Services.

Service profile identifier (SPID)

Acronym for Service Profile Identifier, a number that identifies a specific ISDN line. When you obtain ISDN service, your telephone company assigns a SPID to your line. Part of the initialization procedure is to configure your ISDN terminal adapter to use this SPID.

Most telephone companies in North America use the Generic SPID Format, which is a 14-digit number. The first 10 digits identify the telephone number, called the Directory Number (DN). The remaining four digits identify a particular ISDN device, in the case where multiple devices share the same Directory Number.

Each ISDN BRI line has two telephone numbers. Each of these telephone numbers has a SPID.

services

You can define service schedules for ringing services, restriction services and routing services. This allows you to control call access a different times of the day and for different days of the week.

set

Refers to Norstar digital, IP or ISDN telephones.

Set lock (telephone lock)

This feature allows you to limit the number of features that are available at a telephone. Full set lock allows very few changes or features, Partial set lock allows more changes and features, and No set lock allows any change or any feature. Assign the Set lock under DNXX/Restrictions/Set Restrictions. (Services/Telephony Services/System DNs)

signaling channel

Signaling channels are the communication channels used to send control signals to and from the MSC. Signaling channels are also known as D channels.

Simple Network Management Protocol (SNMP)

SNMP is the protocol governing network management and the monitoring of network devices and their functions.

startup programming

When a Business Communications Manager system is first installed and powered up, you must perform Startup programming before you program other features. Startup initializes the system programming to defaults. Use the Quick Start Wizard to perform this process.

static IP address

A static IP address, or fixed IP address, is an IP address that is permanently assigned to a device on a network. The device retains the same IP address every time it connects to the network and is known to other devices on the network by that IP address.

Station Auxiliary Power Supply (SAPS)

A device which provides power to a telephone that is more than 300 m (975 ft.) and less than 1200 m (3900 ft.) from the Business Communications Manager, or to a CAP module.

Station media bay module

A computer module which provides access to telephone lines within the Business Communications Manager system. The 16-port Digital Station Media Bay Module (DSM 16) connects a maximum of 16 digital telephone sets to the system. The 32-port Digital Station Media Bay Module (DSM 32) connects a maximum of 32 digital telephone sets to the system. The Analog Station Media Bay Module (ASM 8) connects a maximum of eight analog telephony devices to the system. The Unified Manager displays these lines as DN numbers.

station set test

A series of diagnostic tests for these components of a telephone: display, buttons, handset, speaker, and power.

subnet mask

A value used to route packets on TCP/IP networks. When the IP layer has to deliver a packet through an interface, it uses the destination address contained in the packet, together with the subnet mask of the interface to select an interface, and the next hop in that subnet

synchronous

A synchronous signal is sourced from the same timing reference. A synchronous signal causes the interval between successive bits, characters, or events to remain constant or locked in to a specific clock frequency.

Synchronous Dynamic Random Access Memory (SDRAM)

Computer memory that stores data temporarily. SDRAM stores the data used by the microprocessor as it executes instructions. The contents of RAM are erased when you restart or turn off the Business Communications Manager.

system data

An option in the Set Copy function which refers to the programmable system settings that apply to all telephones and lines.

system speed dial code

This two-digit code (01 to 70) allows you to program speed dial codes for the entire system. User speed codes override these settings. Configure system speed dial codes under System speed dial. (Services/Telephony Services)

system startup

See Startup programming.

System-wide call appearance (SWCA)

This feature allows incoming calls to appear as line buttons on all the telephones in the system that either have auto-assigned call buttons or manually-set call buttons set for this feature. When you answer a call with this feature, the next call coming in assigns to the next button. If you specify SWCA hold, as well, when you put a SWCA call on hold, it appears on hold on all telephones where the line appearance occurs.

T

T1

Digital carrier system or line that carries data at 1.544 Mb/s.

T7100 telephone

The Business Communications Manager Business Series Terminal that has a single line display and one programmable button without an indicator.

T7208 telephone

The Business Communications Manager Business Series Terminal that has a single line display and eight programmable buttons with indicators.

T7316 telephone

The Business Communications Manager Business Series Terminal that has a two-line display with three display buttons, 16 programmable buttons with indicators, and eight programmable buttons without indicators.

target lines

Lines used only to answer incoming calls, which routes calls to specific telephones. A target line routes a call according to digits it receives from an incoming trunk. Program target lines under Target lines (Services/Telephony Services/Lines). Assign target lines to sets under DN XXX/Line access/Line assignment. (Services/Telephony Services/ System DNs)

Telephony Application Program Interface (TAPI)

The Telephony Application Program Interface (TAPI) is a standard program interface that lets you and your computer communicate over telephones or video phones to people or phone-connected resources elsewhere in the world.

Telnet

Telnet is a service that provides terminal-emulation capabilities for logging into the Business Communications Manager unit from a remote location.

Terminal Endpoint Identifier (TEI)

A digit used to identify devices using an ISDN connection for D-channel packet service.

token-ring

A token-ring is a network topology and data signaling scheme where a special data packet (called a token) is passed from one station to another along an electrical ring. A transmitting station takes possession of the token, transmits the data, then frees the token after the data has made a complete circuit of the electrical ring.

tone dial telephone

A push button telephone that emits DTMF tones.

transfer

A feature that allows you to redirect a call to another telephone in your Business Communications Manager system, over a network or outside your system. (c 3)

Transfer Callback

If a transferred call is not answered after a specific number of rings, the call returns to the telephone that made the transfer. Transfer Callback does not apply to calls transferred externally. The number of rings is assigned under Timers/Transfer callback timeout. (Services/Telephony Services/General Settings)

Transmission Control Protocol/Internet Protocol (TCP/IP)

A language controlling communication between computers on the Internet.

TCP checks packets of information for errors, sends requests for re-transmission in the event of errors and returns multiple packets of a message into the original sequence when the message reaches its destination.

IP controls how packets are sent out over networks and has a packet addressing method that lets any computer on the Internet forward a packet to another computer that is a step or more nearer to the packet target.

trunk

The physical connection between the Business Communications Manager system and the outside world using the public telephone system or another network system.

Trunk Answer

Use this feature to answer a call on any line that has an active Ringing service Service Mode, when that line does not appear on your telephone. Enable Trunk Answer under Ringing Service/Schedules/<schedule name>. (Services/Telephony Services/Scheduled Services)

trunk media bay module

A computer module which provides access to telecommunications trunks. The Digital Trunk Media Bay Module (DTM) provides the connection between a standard digital PSTN T1 or PRI line and the Business Communications Manager system. The Caller ID Trunk Media Bay Module (CTM) provides the ability to access four (CTM) or eight (CTM 8) analog Caller ID PSTN lines. The Basic Rate Interface Media Bay Module (BRI) provides access to four BRI ISDN telephone lines.

Type of Service (TOS)

The TOS field is located in the IP packet header and is used in DiffServ processing.

U

Universal Dialing Plan (UDP)

Networked systems that connect using UDP have system identification numbers and location codes that are unique to each system, and the DN length is the same. The system identification numbers and location codes are entered as a unique destination code that gets dialed out with whatever extension is being dialed. See also Coordinated Dialing Plan.

unsupervised line

A line for which disconnect supervision is disabled. If an external caller hangs up, the system does not detect the disconnection and does not hang up its line. See Disconnect Supervision.

user data

User Data is an option in the Set Copy feature. User Data refers to the personal settings which are unique to a telephone, and which are not programmed for the system. You program User Data for each telephone.

These settings, for example, include Personal Speed Dial and the assignment of programmable memory buttons.

User Datagram Protocol (UDP)

The UDP is a protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

Like the Transmission Control Protocol, UDP uses IP to actually transfer a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order.

Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

user filter

See Restriction filter.

user preferences

These are settings that define a specific telephone and how the buttons on that telephone are programmed.

User Speed Dial

Two-digit codes (71-94) you program to dial external telephone numbers. You program User Speed Dial numbers for each telephone, and these numbers are available only at the telephone on which they are programmed.

V

V.90

A data transmission standard used by the modem installed in the Business Communications Manager. This standard allows data to be transmitted to the modem at 56 kbit/s and transmitted from the modem at 33 kbit/s.

Voice Call

Use this feature to make an announcement or begin a conversation through the speaker of another telephone in the system. The telephone you call does not ring. Instead, the person you call hears a beep and then your voice. Their telephone will beep periodically to remind the person that their microphone is open. (✆ 6 6)

Voice Call deny

Use this feature to prevent your telephone from receiving Voice Calls.

Voice Message Center

If you have subscribed to Call Display services you can receive visualVoice Message Waiting Indication, providing your telephone has a display. If you haveVoice Message Waiting Indication, you can program the telephone numbers required to access up to five external Voice Message Centers. You can program which of the five Centers is to be accessed by each specific line.

Voice over IP (VoIP)

Voice over IP (VoIP) is the capability to deliver voice traffic using the IP network. VoIP is a set of facilities for managing the delivery of voice information using theIP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

In addition to IP, VoIP also uses the real-time protocol (RTP) to help ensure that packets get delivered in a timely way.

The Business Communications Manager provides VoIP lines that access a gateway on the system. The gateway receives packetized voice transmissions from users within the company and then routes them to other parts of its intranet (local area or wide area network). VoIP trunks can be used by both digital and IP telephones.

W

Wait for dial tone

A feature that causes a sequence of numbers to pause until dial tone is present on the line before continuing to dial. The Wait for dial tone symbol (,) uses two of the 24 spaces in a dialing sequence. This feature requires a Services or Combo Cartridge.

web cache

A web cache is a server or collection of servers that store copies of Internet content. The web cache server can be either located on the LAN where the clients it serves are also located, or it can be embedded within the enterpriseWAN or at the client's Internet Service Provider (ISP).

web proxy

A web proxy, or HTTP proxy, is a server that acts on behalf of the requester of pages from an HTTP server and the Internet.

Weighted Fair Queuing (WFQ)

WFQ is a queuing method that allows low volume traffic such as Telnet to be given priority and interactive traffic receives higher priority than batch transfers. Also, high bandwidth usage traffic such as batch file transfer traffic gets equal priority with other high bandwidth use traffic.

Wide Area Network (WAN)

A collection of computers or Business Communications Managers connected or networked to each other over long distances, normally using common carrier facilities.

wireless

See Companion Wireless.

Index

Numbers

2-way DID, PRI 563

A

access codes 129, 206
acronyms 38
active application DNs 137
active Companion DNs 137
active set DNs 136
Adding a user profile 480
alarm
  codes 514
  CSU 528
  messages 261
  short term 528
  telephone 261, 264
Alarm Backup Batch Job 479
Alarm Banner 481
Alarm Browser 481
alarm data, hospitality 297
Alarm Database 479
Alarm Manager 479
alarm manager settings, overview 481
alarm service settings, overview 415
Alarm time 294
allow last number redial, programming 166
Answer DNs 155
Answer mode 100, 105
antenna type
  Companion 276
application setting options
  Common Open Policy Services (COPS) 463
  QoS
    interface groups 455
    network access 456
    policies (hardware filters) 461
assign
  answer DNs 155
  intercom buttons 152
  line pools 155
  lines 152
auto attendant, adding a set 141
auto DN, programming 112
automatic route selection (see call routing)
automatic telephone relocation, programming 531
aux ringer
  hunt groups 287
auxiliary ringer
  programming 100
  troubleshooting 544

B

back up WAN 341
Background music 260, 264
  troubleshooting 544
BRI (Basic Rate Interface) module 563–565
  line types 583
BRI (see also ISDN)
Business Communications Manager
  IP Routing information protocol 375
  logging off 55
  logging on 51
  rebooting 553
  WAN connections, permanent
    frame relay 326
    PPP 326
  with Meridian M1 over PRI 211
Business Communications Manager ATA 2,
  troubleshooting 543
Business Communications Manager system networking 198
button programming
  features list 593

C

call buttons
  SWCA 263
Call by Call
  example 208
  PRI limits 188
  programming service selection 188
  routing table 120
  service selection 83
Call Center, active DNs 137
call log
  automatic 153
  password 150
  set 153
  space 169

Call Offer 239
Call Permission 296
Call routing
  programming 117
  tandem networks 217
called ID 169
Caller ID
  by region 577
calls
  auto-assign SWCA calls 263
Camp timeout delay 265
CAP (Central Answering Position)
  line assignment 154
  programming 174
card edge loopback test 524
carrier access codes 115
carrier failure alarms 526
Caution symbol 36
CbC routing table example 120
CbC, routing information 209
cell assignment, Companion 276
Central America, supported languages 576
central answering position (see CAP)
change DNs 140
Channel Service Unit (see CSU)
CLASS assignment 169
Class of Service (see COS)
clock source
  about 80
  master 81
  primary reference 80
  secondary reference 80
CO fail 82
Common Open Policy Services (COPS)
  about 463
  viewing capabilities and statistics 463
common set, Hospitality 294
common settings 250
companding laws, by region 577
Companion
  active DNs 137
  antenna type 276
  cell assignment 276
  enable handset registration 274
  handset credits 274
  radio ID 276
  register handset 274
  registration password 274
  supporting regions 579
  troubleshooting 553
  UTAM approval 274
Companion programming
  cell
    neighbours 277
    radio neighbour 277
    radios 277
  disabling registration 274
  enabling registration 274
  recommended settings 278
  re-evaluation 276
  re-evaluation status 276
Configuring an ISDN interface 342
configuring management settings
  alarm manager, overview 481
  user manager, overview 479
configuring resource settings
  LAN 320
  WAN backup links
    access parameters 341
    link parameters 340
    overview 338
  WAN primary links
    frame relay parameters 331
    line parameters 330
    overview 326
    performance graphs and tables 337
    PPP parameters 335
    sync parameters 331

configuring service settings
alarm service, overview 415
DHCP
LAN 357, 369
overview 354
Remote Scope 363
DNS, overview 372
NetLink manager, overview 412
QoS monitor
mean opinion score 408
overview 408
routing, overview 374
SNMP
community list 404
manager list 405
trap community list 406
TAPI Service Provider, overview 415
voice record, overview 415
VoIP Gateway, overview 408
Web cache, overview 410
configuring system settings
fault alarm banner 535
performance graphs and tables 535
connecting to Business Communications Manager, methods for
remote dial-in 350
connections, stand alone 565
Contrast Adjustment 536
Conventions and symbols 36
coordinated dialing plan 198
copy telephone settings 148
copyright 2
cordless handsets 281
core software, regions 575
COS (Class of Service)
auto DN 112
calls answered with DISA 112
password 184
auto-answer system 131
line restriction 185
user filter 185
with DISA 180
credits, Companion handset 274
CSU (Channel Service Unit)
alarms 528
description 83
performance statistics 527
stats 526
CSU (Channel Service Unit) line build 82
customizing call display services 169

D

Danger symbol 36
DECT 281
DNs 138
supporting regions 579
defaults
dialing restriction 194
directory number lengths 176
restrictions 194
set restrictions 167
delay
Camp timeout 265
Delayed Ring Transfer 261, 265
Park timeout 265
Transfer callback 265
Delayed ring transfer 261, 265
Deleting a user profile 481
Deleting an ISDN interface 345, 349
deprovisioning a line 86
destination code, description 118, 122
device
disabling 510
enabling 510
DHCP service settings
LAN 357, 369
overview 354
Remote Scope 363
diagnostics 498
T1 signal 526
test results, system test log 511
dial tone absent on external lines 538
Dialing plan
coordinated 198
PRI 563
PRI routing table 121
shared line pools 206
using T1 E&M lines 203

dialing restriction
defaults 194
exceptions 191
for remote callers 104
line filter 185
line/set restriction 167
maximum length 191
remote 192
remote user 104
removing a filter 191
Restriction service 190
restrictions 191
set restrictions 165
user filter 185
wild card character 122, 193
DID (Direct Inward Dial) trunk 132
Digital Trunk Interface (see DTI)
Direct dial digit, programming 112, 177, 261
Direct Inward Access
lines in a network 247
Directed pickup 261, 265
directory numbers
coordinated dialing plan 198
length 176
DISA (Direct Inward System Access)
DID, trunk 132
DN 112
remote callers 180
disable handset registration 274
disabling
a device 510
a module 508
disconnect supervision
loop start trunks 131
display unreadable, troubleshooting 537
distinct ring
hunt groups 288
distinct rings in use, hunt groups 287
Diversion 236
DN hunting (see multi-line hunt)
DNs
changing 140
line access 150
renumbering wizard 139
DNS guidelines 372
DNS service settings, overview 372
DPNSS
remote access 132
DPNSS 1 features 235
DSCP Mapping Modification page 460
DSCP Mapping Table page 460
DSX1 build 82
DTI (Digital Trunk Interface), trunk 202
DTM
clock source 80
LEDs 546

E

E1 CALA 575
E1 Euro 575
E1 Global 575
Edit Template Wizard 140
enable handset registration 274
enabling a module 509
Enbloc dialing 128
error messages
10.5.2 502
11.12.10 502
11.19.9 502
11.5.2 502
14.17.40 502
14.17.41 502
14.17.68 502
14.4.21 502
14.5.77 503
2.5.4 500
2.5.6 500
2.5.8 500
2.xx.4 500
2.xx.6 500
5.16.68 501
5.4.59 500
5.5.39 500
5.5.40 500
5.5.41 501
5.5.45 501
8.4.2. 501
8.5.3 501
8.8.3 501
9.4.2 501
9.6.4 501
9.6.5 501
9.6.6 501
overview 499
Telephony programming is currently not available 56, 74, 498
user actions 499

Ethernet
WAN connections, permanent
frame relay 326
PPP 326
evening schedule 251
event messages
maintenance 515
significant 515
system restarts 518
exception (see dialing restriction)
expired alarms, hospitality 298
extended superframe 82
external code, programming 112
external lines, access code 113
external paging, troubleshooting 544
extra-dial telephone, programming 254

F

Fast 321
Fast Routing 321
fault alarm banner settings 535
feature
button programming 593
codes, troubleshooting 550
using remotely 131
Feature Settings
access codes 129
Call log space 264
CAP assignment 174
Direct dial 177
Held reminder 261, 265
page 265
page tone 261, 264
SWCA Control 263
filtering
criteria 556
ranges 556
filters (see also restriction service) 167, 190
filters, room restriction 296
first display 169
frame relay 326
frame relay parameters, WAN 331
framing format 82

G

General Settings
Feature Settings 260
Remote Access 183
Global 575

H

handsets
DECT 281
registering 274
Hold
tones, music, or silence 260, 264
hold
hold
auto hold control 157
invoked by hold, SWCA feature 263
Home Location Code 245
hospitality
configuring 295
expired alarms 298
types of sets 294
hospitality admin set 294
hung lines 539
Hunt Groups
about 285
Assigning lines 290
Broadcast mode 286
Distribution modes 286
Moving members 289
Rotary mode 287
Sequential mode 287
Unassigning lines 290
usage metrics 530
hunt groups
auxiliary ringer 287
disctinct rings 288
disctinct rings in user 287

I

ICMP counters 504
idle line, search for 102
impedance, setting for line 102
inactive DNs 137
interdigit timeout 180
interface levels 82
internal CSU 83

internal numbers
coordinated dialing plan 198
length 176
Intrusion Capability Level 238
Intrusion Protection Level 238
IP Routing 374
information protocol 375
ISDN (Integrated Services Digital Network)
bearer capability 559
BRI card 563–565
capabilities 557
capability packages 568
capability packages, ordering 566
clocking 565
data transmission speed 560
DNs 138
installation programming 569
layers 558
line services, by region 578
network synchronization 565
ordering service 568
planning service order 558
programming sequence 569
S interface 564
S reference point 564
services and features 560
SPID 573
standards 566
T reference point 564
terminal equipment configuration 564
ISDN Access Parameters 344
ISDN Channel Characteristics 344
ISDN loss plan setting 82
ISDN Overview 557
ISDN PRI
2-way DID 563
Dialing Plan 563
ISDN Summary 342

K

keycodes
DECT 281

L

LAN performance 325
LAN resource settings 320
LAN, DHCP settings 357, 369
language
by region 576
South and Central America 576
LEDs, DTM 546
line
assignment 152
BRI and PRI line types 583
control sets 96, 105
deprovisioning 86
pool
access codes 114, 206
troubleshooting 551
programming
name 96, 105
telco features 103
trunk/line data 97
protocol by region 582
provisioning 86
restriction programming 103
selection, for a direct dial telephone 177
troubleshooting 537–542
line access, System DNs 150
line coding 82
line parameters, WAN 330
line pool access code 114
line protocol, by region 582
line restriction 190
line services
ISDN support, by region 578
line/set restriction 167, 190
user filter 185
link parameters, WAN 340
Link time 265
log
network evt 513
space
programming 169
system administration 512
system test 511
logging off of Business Communications Manager 55
logging on to Business Communications Manager 51
Loop avoidance, programming 244
loop start trunk
remote access from public network 131
loopback test, starting 524
loss package 102
loss/gain settings 102
lunch schedule 251

M

M7324 telephone
CAP 174
mailbox
add through wizard 141
maintenance
alarm codes 514
bipolar violations 528
carrier failure alarms 528
CSU stats 526
disabling module/cartridges 508
enabling the module 509
event messages 515
identify device connected to system 509
network event log 513
programming
system administration log 512
short term alarms 528
system
administration log 512
test log 511
version 507
Management 479
MCDN
private networking 211
MCDN network 219
mean opinion score, QoS monitor 408
media bay modules
availability by regions 580
Media Bay Modules, clock source 80
Meridian, MCDN network 219
message centre, selecting 243
Message Waiting Cancellation 241
Message Waiting Indication 241
Message Waiting Indication, setting 244
Message, sending 261
MIB-II
counters 503
variables 503
mobiles
by region 579
Modem Link Parameters 340
Modifying a user profile 480
module
enabling 509
showing inventory 508
troubleshooting 552
moving telephones (see automatic telephone relocation)
multi-line hunt 560
groups 568
MWC 241, 243
MWI 241, 243

N

National ISDN standards 566
NetLink manager settings, overview 412
network
configuration samples 197
event log 513
private systems to Business Communications Manager 198
public network to Business Communications Manager 198
troubleshooting 548–552
user problems 548
network access, configuring IP filters 456
Network Name Display 129
calling party name 130
interactions 130
networks
MCDN 219
SL-1 211
tandem 212
night schedule 251
No free lines 542
Not available 541
Not in service 541
NSI string 243
NT1 (network termination type 1) 566
stand alone connections 565

O

On hold (see hold)
optional equipment, troubleshooting 543–544
outbound traffic filter, creating 555
Outgoing name and number blocking 270
overflow routing 256

P

packet filtering
features
protocol 473
source address 473
source mask 473
Paging, remote 133

Park
retrieving calls 112
timeout delay 265
park prefix 112
password
calls answered with DISA 112
Companion 274
COS 184
service control 250
using DISA 180
payload loopback test 523
performance 498
performance graphs and tables
system 535
WAN 337
Point to Point Protocol (PPP) 326
policy-enabled networking 447
actions 451
DiffServ 447
DiffServ Code Point (DSCP) 447
filters 451
policy 451
portable services
supporting regions 579
portable systems, DECT 281
portable telephone
disabling 274
enabling 274
troubleshooting 553
PPP parameters, WAN 335
PPPoE Access Parameters 348
PPPoE Channel Characteristics 349
PPPoE Summary 347
PRI
line types 583
SL-1 networking 219
PRI line pools 189
PRI line, provisioning 85
PRI Networking
Call-by-call services example 208
Meridian M1 configuration 219
primary WAN connection 413
prime telephone 261
Private Access Code 245
private line 98
private network 201
PNTC call routing 215
remote access 131
private networking with PRI 211
programming
alarm telephone 261, 264
allow last number redial 166
auto DN 112
call routing 117
CAP assignment 174
features on a set 169, 255
General Settings 259
ISDN 569
least cost routing 127
line access 150
lines 91–106
maintenance 497–529
on lines
dialing restrictions 255
ISDN (BRI) lines 571
ISDN (PRI) lines 571
trunk/line data programming 97
services 189–251, 268, 271
system 175
System DNs 135–169
system features
auxiliary ringer 254
called ID 169
CLASS assignment 169
DN length 176
extra-dial telephone 254
log space 169
remote restrictions 104
restriction service 165–168, 190, 255
ringing 253
schedule times 251
System Speed Dial 267
telco features 103, 165
trunk answer 253, 254
system speed dial 267
Telco Features 269
Programming PRI routing table 121
protocols, routing information 375
provisioning, T1 lines 85
public line 98
public network
PNTC routing 213

Q

QoS
about 453
defined filters, installing 461
interface groups
configuring 455
deleting 455, 456
IP filter groups
about 456
configuring 458
modifying 459
IP filters
about 456
configuring 456
policies, configuring 461
role combinations
deleting 455, 456
QoS best effort queue counters 506
QoS best effort traffic counters 506
QoS dropped packets counter 506
QoS graph counters 506
QoS monitor settings
mean opinion score 408
overview 408
QoS session counters 505
Quick Start Programming Wizard 59

R

radio ID 276
reallocating log space 264
rebooting Business Communications Manager 553
Received number length 176
receiver volume 260, 264
re-evaluation, see Companion programming
regions
caller ID 577
companding law 577
core software 575
ISDN line services support 578
languages 576
line protocol 582
mobility services 579
modules 580
system defaults 586
voice mail 589
voice mail feature defaults 589
registering Companion handsets 274
registration
on a portable 277
registration password 274
regulatory information 2
remote
filters 185
system access 131–132
users, troubleshooting 548–552
remote access
dialing restriction 190
DID trunks 132
DPNSS 132
from public network 131
loop start trunks 131
on a private network 131
PRI trunk 132
restricting 183
T1 E&M trunks 131
remote dial-in, guidelines 350
Remote Paging 133
remote restriction 192
remote routers, setting up 555
remote system access 131
restricting
line at telephone 167
lines 103
remote access 183
remote callers 104
telephones 165, 190
restriction
default 167
dialing 128
service 103, 165, 255
line/set 165, 167
programming 255
schedules 167
service control password 250
Restrictions, using 190
retrieving voice messages 269
ringing service
night schedule 253
ring group assignment 253
ringing groups 253
room restriction filters 296
room set
Hospitality 294
identifying 296

Route
adding a long distance access code 126
dialing plan to route outgoing PRI calls 128
dialing restrictions 128
for least cost routing 127
for local calling 124
for long distance calling 125
routing
CbC services routing 209
destination codes 118
dialing restrictions 128
sample for local calling 124
sample for long distance calling 125
settings 374
tandem networks 217
routing schedules
service control password 250
routing, IP
information protocol 375
managing information 374

S

S interface 564
S or T reference point 564
S reference point 564
Schedule 4 251
Schedule 5 251
Schedule 6 251
security, dialing restriction 190
service control password 250
services
evening 251
example of alternate call ringing 252
lunch 251
night 251
programming
common settings 250
restriction services 255
ringing groups 253
ringing service 253
programming ringing sets 254
Schedule 4 251
Schedule 5 251
Schedule 6 251
schedule times 251
services routing 209
set
feature and number restrictions 165
restriction
default 167
user filter 185
Setting global WAN parameters 327
setting up
logging off of Business Communications Manager 55
logging on to Business Communications Manager 51
rebooting Business Communications Manager 553
significant event messages 515
SL-1
MCDN network 219
tandem network 212
SL-1 networking 211
SNMP guidelines 403
SNMP service settings
community list 404
manager list 405
trap community list 406
SNMP Trap 479
South America, supported languages 576
speed dial 267
Speed Dial programming 267
start and stop times, services 251
Static routes 377
statistics 498
superframe 82
SWCA
auto hold control 157
auto-assign call button 263
invoked by hold 263
Symbols 36
sync parameters, WAN 331
system
administration log 512
processor software 507
sample configurations 197
speed dial 267
test log 511, 515, 518
version 507
system defaults, by region 586

System DNs
allow redirect 158
answer DNs 155
auto hold 157
auxiliary ringer 157
capabilities 157
direct-dial 157
DND on busy 157
handsfree 157
handsfree answerback 157
headings 135
hotline 159
intercom keys 152
line assignment 152
line pool access 155
page zone 157
paging 157
pickup group 157
priority call 157
redirect ring 158
restrictions 165
telco features 165
user preferences 162
system performance graphs and tables 535

T

T reference point 564
T1
signal diagnostics 526
transmission performance 526
T1 Etiquette 575
T1 parameters
CO fail 82
CSU line build 82
DSX1 build 82
Framing 82
Line coding 82
T1CT2 Plus 575
T7100 telephone
accessing external lines 112
tandem networking 212
call routing 217
target lines
description 202
TCP counters 505
TE (see ISDN terminal equipment)
telephones
adding a set to the Auto Attendant 141
button features list 593
control sets 149
direct dial 112
Edit Template Wizard 140
line access 150
log calls automatically 153
troubleshooting 536
voice message waiting indication 153
Telephony programming is currently not available 56, 74, 498
telephony, system DNs headings 135
testing
loopback tests 523
system test log 511
Three Party Service 235
time zones, by country 585
tip 36
toll-free, tandem networks 212
trademarks 2
traffic, classifying 456
Transfer callback 265
troubleshooting 533
auxiliary ringer 544
background music 544
Business Communications Manager ATA 2 543
external paging 544
line pools 551
lines 537
modules 545
network or remote users 548–552
optional equipment 543–544
portable telephone 553
T1 signal 547
Telephony programming is currently not available 56, 74, 498
trunk modules 545, 547
types of problems 534
trunk
answer, programming 254
DTI 202
module, troubleshooting 545, 547
numbering 202
types 202
trunk/line data 97

U

UDP counters 505

Usage metrics, Hunt groups 530
User Manager 479
user manager settings, overview 479
user preferences
  button features list 593
User Profile 479
user profile warning 59
UTAM 274
utilities, overview 498

V

V.90 modem interface 339
voice mail
  active DNs 137
  add subscriber mailbox 141
  feature defaults, by region 589
  regions 589
voice message
  accessing 153
  external center 269
  waiting indication 153
voice record, service settings 415
VoIP Gateway 342
VoIP gateway settings
  overview 408

W

WAN connections, permanent
  frame relay 326
  PPP 326
WAN Overview 326
WAN resource settings
  backup links
    access parameters 341
    link parameters 340
    overview 338
  primary links
    frame relay parameters 331
    line parameters 330
    overview 326
    performance graphs and tables 337
    PPP parameters 335
    sync parameters 331
warning 59
Warning symbol 36
Web cache settings, overview 410
web caching/proxy, guidelines 410
wild card character 122, 193
Windows NT login sessions warning 60
wireless
  DECT 281
wiring, loopback test 523
Wizard Instance Timeout Message 60
wizards
  Edit Template Wizard 140
  renumbering DNs 139